

DEFENDANTS' EXHIBIT 70:



Twitter: Response to Request for Information

Twitter's mission is to elevate the public conversation online, and we take our responsibility seriously. Since the onset of the coronavirus pandemic, Twitter has worked hard to elevate credible information from reliable third-party voices and address harmful misleading information about COVID-19. We appreciate the opportunity to share some of our work in response to the Request For Information.

We have continually refined our approach as we have learned more about the causes and treatments of COVID-19. We have a two-pronged approach: elevating credible information about the novel coronavirus and addressing misinformation about the pandemic.

Throughout these unprecedented times, Twitter has continued to adapt and update both policies and enforcement, as well as increase transparency and share more data to ensure experts and the public can better analyze how discussion around COVID-19 continues to evolve. We have kept an updated blog with all relevant information on Twitter's efforts covid19.twitter.com, and to date, **over 160 million people have visited the COVID-19 curated page, over two billion times.**

We have taken several steps to promote reliable public health information, including by creating a [dedicated COVID-19 Hub](#) in our #Explore tab with reliable, human-curated information for all 50 states.

We also launched creative engagement tactics including #WearAMask and #Vaccinated 🙌 campaigns to promote public health. We've worked with key partners in and outside of government, including the Civic Nation, the AdCouncil, the Department of Health and Human Services (HHS), and the Black Coalition Against COVID to supply the public with reliable information about the coronavirus, treatments, and vaccines. Since 2020 we have supplied partners with more than \$2.5 million in in-kind ad credit through our Twitter Ads for Good program. And, once vaccines became widely available to all adults, we created a search prompt, so that the first result for common coronavirus vaccine search terms was a link to vaccines.gov.

Since the beginning of the pandemic, we've prioritized [addressing misleading claims](#) that could lead to offline harm. In March 2020, we began removing Tweets that advanced debunked claims about the causes and treatments of COVID-19, including, for example, that 5G cell towers caused infection or that consuming bleach cured it. With the advent of vaccines in late 2020, we updated our policies to clarify we would take action on specific false claims about the pandemic, including many conspiracy theories, claims about the efficacy of the approved vaccines, and more.



[In early 2021](#), we introduced a [strike system](#) to determine, and further clarify to the public, when enforcement action is necessary. We believe this system helps to educate people using Twitter about how we enforce our rules, while reducing the spread of potentially harmful and misleading information.

Tweets labeled in line with [this policy](#) have limited visibility across search, replies, and on timelines, and they aren't recommended algorithmically by Twitter, further reducing the content's spread.

So far, [the vast majority of content we take action on for misinformation is identified proactively](#) — either through automation (accounting for more than 50% of all enforcements) or proactive monitoring.

Earlier this year, we began testing a [new label design](#) that includes additional context about why a Tweet may be misleading — we've since rolled these redesigned labels out to more people. In our test, more people clicked into the new labels and fewer people Retweeted or liked potentially misleading Tweets with these labels. We'll continue to improve our label design.

Below is an overview of the measures we have taken to protect the health of the public conversation while ensuring we are a collaborative and open partner in endeavors to address the challenging and changing online and offline issues society is facing.

Continuing to build on our commitment to **sharing meaningful insights of our work**, we've published [the latest update to our Twitter Transparency Center](#) with relevant data from 1 January 2021 to 30 June 2021.

One of our key findings was on enforcement: Twitter required account holders to remove 4.7M Tweets that violated the [Twitter Rules](#). Of the Tweets removed, 68% received fewer than 100 impressions prior to removal, with an additional 24% receiving between 100 and 1,000 impressions. In total, impressions on **these violative Tweets accounted for less than 0.1% of all impressions for all Tweets** during that time period.

Below you will find additional metrics about our COVID policy enforcement.



COVID-19 Guidance Enforcement

Since introducing our [COVID-19 guidance](#) in 2020, our enforcement teams have challenged 11.7 million accounts, suspended 6,599 accounts and removed over 77,287 pieces of content worldwide.

Overview in numbers: Violations of our COVID-19 misleading information policy

2021	January	February	March	April	May	June
Unique accounts suspended (globally)		48	149	260	185	156
Pieces of content removed (globally)		6822	5371	5091	5147	5117
2021	July	August	September	October	November	December
Unique accounts suspended (globally)	215	229	254	819	431	666
Pieces of content removed (globally)	6602	5579	4544	3574	4129	4559

2022	January	February
Unique accounts suspended (globally)	2153	336
Pieces of content removed (globally)	3397	1828

In the month of January, we suspended 2,153 accounts and removed 3,397 pieces of content globally, whereas in the month of February, we suspended 336 accounts, and removed 1,828 pieces



of content globally for violation of our [COVID-19 misleading information policy](#). As the conflict in Ukraine has escalated, it has become a key priority for our internal teams, shifting attention away from COVID-19 to current events in Ukraine, as reflected in the numbers above.

Advertising on COVID-19

Twitter has a strict advertising policy on COVID-19, the details of which can be found [here](#).

Overview in numbers: Violations of our COVID-19 advertising policy

2021	January	February	March	April	May	June
Number of promoted Tweets that violated Twitter's COVID-19 policy	864	977	945	869	745	729
2021	July	August	September	October	November	December
Number of promoted Tweets that violated Twitter's COVID-19 policy	338		84		64	

2022	January	February
Number of promoted tweets that violated Twitter's COVID-19 policy	34	37

Research and data access

Twitter is the largest source of real-time social media data, and we make this data available to the public for free through our [public API](#). Our service is industry-leading in this regard. You can [find out more here](#).

To further support our ongoing efforts to protect the public conversation, and help people find authoritative health information around COVID-19, Twitter released a [specific COVID-19 API endpoint](#) into Twitter Developer Labs to enable approved developers and researchers to study the public conversation about COVID-19 in real-time. These researchers have published important findings that have advanced the public understanding of the pandemic. For example:

- In February, a **Yale scientist launched a study into how social media led to long COVID discovery**. [Akiko Iwasaki's active Twitter use might have led her to the treatment for long COVID](#) after finding a Facebook poll made by individuals with the condition. Iwasaki highlighted the value



of Twitter's role in science, allowing a direct line of communication between scientists and patients.

- Over 100 researchers and developer teams, representing 92 different academic institutions and universities around the world were granted access to the COVID-19 data stream we made available.
- More than half of those approved for this stream are **focused on studying disinformation and misinformation around the facts of coronavirus**, see examples in [previous reports](#) under "How researchers studied COVID-19 on Twitter."
- Since the Twitter API was introduced, academic researchers have used data from the public conversation to study topics as diverse as the conversation on Twitter itself, including [attitudes and perceptions about COVID-19](#) and [efforts to promote healthy conversation online](#).

As of: July 15, 2022
Received: May 02, 2022
Status: Pending_Post
Tracking No. l2p-5r8z-rkjd
Comments
Due: May 02, 2022
Submission Type: Web

PUBLIC SUBMISSION

Docket: HHS-OASH-2022-0006

Impact of Health Misinformation in the Digital Information Environment in the United States Throughout the COVID-19 Pandemic

Comment On: HHS-OASH-2022-0006-0001

Impact of Health Misinformation in the Digital Information Environment in the United States Throughout the COVID-19 Pandemic

Document: HHS-OASH-2022-0006-DRAFT-0418

Comment on FR Doc # N/A

Submitter Information

Email: toboyle@twitter.com

Organization: Twitter

General Comment

Twitter is grateful for the opportunity to submit this response to the Request for Information. Please address any questions about our response to toboyle@twitter.com

Attachments

Twitter Response to USSG RFI



**Response to Surgeon General VADM Murthy's Request for Information:
Health Misinformation
HHS-OASH-2022-0006-0001**

May 02, 2022

Google appreciates the opportunity to submit comments in connection with the U.S. Surgeon General's Request for Information on the "Impact of Health Misinformation in the Digital Information Environment in the United States Throughout the COVID-19 Pandemic." Since the outbreak of COVID-19, teams across Google have launched more than 200 new products, features, initiatives and are contributing more than \$1 billion in resources to help our users, clients, partners, and governments through this unprecedented time. Our major efforts are focused around: providing trusted information to our users, helping people adapt to a changing world, and contributing to recovery efforts across the globe. This submission details our efforts to provide high quality information to help keep people safe during the COVID-19 pandemic.

Our Approach to Addressing COVID-19 Health Misinformation and Disinformation

Google and YouTube work to make it easy for people to find accurate and up-to-date information, especially in times of crisis. Since the outbreak of COVID-19, teams across Google have worked to provide quality information and resources to help keep people safe, and to provide public health, scientists and medical professionals with tools to combat the pandemic. We were able to act quickly and decisively because of the significant investments we have made over years, not only to make information useful and accessible, but also to remove and reduce the spread of harmful misinformation.

Across all of this work, we strive to have clear and transparent policies and enforce them without regard to political party or point of view. This includes long-standing [policies](#) prohibiting harmful and misleading medical or health-related content. We work to raise up authoritative sources, and reduce the spread of misinformation in recommendations and elsewhere. Teams across the company work in a variety of roles to help develop and implement our policies, monitor our platforms for abuse, and protect users from everything

from account hijackings and disinformation campaigns to misleading content and inauthentic activity. And we don't do this work alone; we work closely with experts to stay ahead of emerging threats.

Promoting Authoritative Content

Over the course of the pandemic, interest in COVID-19 has been high around the world. In response, we have worked to help people find the information they need across Google and YouTube – including by partnering with health organizations and governments to bring our users authoritative information in a rapidly changing environment. In addition to this work, we launched a [website](#) in over fifty countries that provides resources dedicated to COVID-19 education and prevention.

- In [Search](#), in response to the pandemic, we originally introduced a comprehensive experience for COVID-19 that provided easy access to information from health authorities alongside new data and visualizations. This format organized the search results page to help people easily navigate resources. This experience complemented pre-existing work on Google Search and Google News to recognize sensitive events and contexts, as our systems are designed to elevate authoritative sources for those classes of queries. We're continually investing in Search to make sure that the information people get is relevant and reliable. Finally, we've worked with authorities to surface additional information to help users learn about and find COVID vaccines. We surface a list of U.S. Food and Drug Administration (FDA) authorized and approved COVID vaccines and information from the U.S. Centers for Disease Control and Prevention (CDC) or FDA about those vaccines. We surface COVID vaccine locations based on the vaccines.gov database, and a national website and phone number for users to get more information.
- On the [Google HomePage](#), in partnership with the World Health Organization and other health authorities, we have promoted important guidance to prevent the spread of COVID-19. The efforts, including prevention tips and messaging on our homepage, have launched in more than 100 countries to date.
- Across [YouTube](#), we are raising up authoritative sources such as the World Health Organization (WHO) and local public health authorities to help users obtain the latest COVID-19 information in search results and recommendations. We have displayed information panels linking to global and locally relevant health officials on our homepage, and in panels that appear on videos and searches about COVID-19. When a user in the U.S. watches a video about COVID-19, we display an information panel that points to the CDC's official resource for information about COVID-19 and the Google search results page with health information from the CDC and local statistics and guidance. In early 2021, we added a vaccine-specific information panel so that when a

U.S. user watches a video about COVID-19 vaccines, we show a panel that points to the CDC's online resource for vaccine information, with an additional link to the Google search results page with information about vaccination. We have also donated advertising inventory to governments and NGOs to help give their public health messages about COVID-19 more visibility on YouTube. In addition, YouTube elevates content from authoritative channels such as news organizations or health authorities in the search results for certain health-related queries. We have also curated and elevated playlists containing content from community organizations and paired popular creators with public health experts to reach a diverse set of users across our platform—including with content in Spanish.

- In [Google News](#), as the pandemic was breaking, we created a new COVID-19 section with links to up-to-date, relevant stories from the international to local levels from a variety of authoritative sources. The section puts local news front and center by highlighting stories about the virus from local publishers in the reader's area.
- We continue to elevate the work of [fact-checkers](#) in **Google Search, Google News, and Google Images**. This means that we label certain articles that have been written by fact-checkers and have used the [ClaimReview](#) markup. In other words, when a user searches for a query and the Search results page includes articles that are fact checking articles, we will label them as such. In order for an article to be eligible to display these "snippets" on the Search page, site publishers need to use [ClaimReview](#) markup so that we can detect that their content is a fact check and ensure they meet our eligibility criteria and technical guidelines, which are outlined [here](#). While this effort began before the COVID-19 pandemic, we have observed that many fact-checkers have elected to focus on health misinformation over the course of the pandemic. YouTube also offers a fact-check panel in search results, which draws content from third party fact-checking sources and may trigger on search results for queries related to misinformation-prone topics.
- On [Google Maps](#), we made it easier to find authoritative information about local health resources, including COVID-19 testing sites, vaccination locations, shelters, general mask availability, food banks and virtual healthcare options where available. We also used authoritative data sources to display COVID-19 cases in a particular area, and whether numbers were going up or down. Since launching our COVID-19 vaccination information panels in 2020, we've provided authoritative COVID vaccine information to people in over 200 countries across dozens of languages. In addition, Maps displays updated information about whether local businesses changed during COVID-19 or offered limited services like take out or curb-side pick-up. We increased our focus on enforcing user review policies— including taking down irrelevant content or misinformation related to COVID-19. We worked with public health officials and other

authoritative sources to show vaccination site information. We also worked with businesses to make safety protocol information more clear for patrons. We are still working to ensure our information is up to date to reflect updated business hours, closures, etc.

- On [Google Play](#), we prioritize the review and publication of policy-compliant apps published, commissioned or authorized by official government entities and public health organizations. Authorized COVID-19 apps must comply with all [Play Developer policies](#), including User Data, Permissions, and Malicious Behavior. We also launched a “stay informed” page in the Play Store with apps that can help users stay informed and prepared during the crisis, using authoritative sources such as the WHO app. Play is also prioritizing a speedy review and approval of Exposure Notification apps – we refer interested governmental public health entities to apply via the publicly available intake form. We also clearly mark trusted official Exposure Notification apps for users to identify.
- Through our [Ad Grants Crisis Relief program](#), Google.org has committed over \$800 million to help more than 100 local government agencies and global non-governmental organizations run critical public service health announcements. In the US alone, Google.org has donated \$59M in Ad Grants, serving 309M public service announcements.

Taking Action Against Misinformation

In addition to elevating authoritative information, we remove COVID-19 related misinformation that contradicts guidance from health authorities and may result in real-world harm.

- On **YouTube**, our Community Guidelines prohibit content about COVID-19 that poses a serious risk of egregious harm and that spreads medical misinformation that contradicts medical information about COVID-19 from the WHO or local public health authorities. As medical and scientific understanding of COVID-19 situation and related public health guidance has evolved, we have partnered closely with international, federal and local public health authorities to ensure our policy definition and enforcement is effective. This work on YouTube has evolved into a comprehensive [COVID-19 medical misinformation policy](#), which prohibits, for example, content that denies the existence of the coronavirus or encourages the use of home remedies in place of medical treatment. We further expanded this policy to include a set of COVID-19 vaccine-related claims that contradicts expert consensus from US public health authorities or the WHO. For example, we remove content with claims that an approved COVID-19 vaccine will kill people who receive it. As of March 31, 2022, we have removed more than 300,000 videos for violating the vaccine provisions of our COVID-19 misinformation policy.

- On **Google Search**, our [medical content policy](#) applies to information we've highlighted in Search features, including those that relate to COVID-19. We don't allow content that contradicts or runs contrary to scientific or medical consensus and evidence-based best practices. If content appears in Search features and violates this policy, we reserve the right to remove the information from the feature.
- On **Google Play**, our policies prohibit developers from capitalizing on sensitive events. Our long-standing content policies strictly prohibit apps that feature health-related content or functionalities that are misleading or potentially harmful, including about COVID-19. Apps that violate these policies may be removed.
- On **Maps**, our policies prohibit misinformation about prevention, transmission and treatment services, as well as allegations that an individual contracted COVID-19 at a particular location. These types of contributed content will be removed.
- On our **advertising services**, we have a wide range of policies to protect users and the ads ecosystem at large from misinformation and disinformation. For instance, our policies for both [publishers](#) and [advertisers](#) prohibit monetization of content that promotes "harmful health claims" or that "relates to a current, major health crisis and contradicts authoritative scientific consensus". Under this policy, for example, we demonetize publisher content that includes claims about the propagation of COVID-19 that contradict the WHO guidance, such as theories involving 5G towers as a transmission vector. In addition, the COVID-19 crisis has been treated as [a sensitive event](#) under Google Ads policy as of January 2020. Under this policy, we do not allow ads that potentially profit from or exploit a sensitive event with significant social, cultural, or political impact, such as civil emergencies, natural disasters, public health emergencies, terrorism and related activities, conflict, or mass acts of violence (please see here for the [latest updates](#) under this policy with regards to COVID-19) We have blocked or removed over 286 million coronavirus-related ads (globally) since January 2020, including Shopping ads, for policy violations including price-gouging, capitalizing on global medical supply shortages, making misleading claims about cures, and fake vaccine doses.

Supporting Initiatives to Increase User Awareness

Helping the world make sense of information during a health crisis requires a broad-based response, involving scientists, journalists, public figures, technology platforms and many others. As such, we also outline in this section our initiatives to support user awareness beyond direct interactions with our services, e.g. via partnerships with or support for relevant third party organizations. Those include:

- Supporting coronavirus fact-checking and verification efforts through more than [\\$6.5 million in funding from the Google News Initiative](#) to fact-checkers and nonprofits fighting misinformation around the world, with an immediate concentration on COVID-19, to several organizations including Correctiv, Maldita.es, Full Fact, First Draft and Science Feedback in Europe. In addition, we're working to increase access to data, scientific expertise and fact checks through support for collaborative databases and providing insights to fact-checkers, reporters and health authorities including sharing [localized data](#) from Google Trends on COVID-19 down to the city level.
- The Google News Initiative provided an additional \$1.5 million to fund the creation of a COVID-19 Vaccine Media Hub and support new fact-checking research.
 - Led by the Australian Science Media Centre, and with support from technology non-profit Meedan, the hub will be a resource for journalists, providing around-the-clock access to scientific expertise and research updates. The initiative includes science media centers and public health experts from Latin America, Africa, Europe, North America and the Asia-Pacific region, with content being made available in seven languages. It has been [up and running](#) since March 2021.
 - To better understand what type of fact-checking can effectively counteract misinformation about vaccines, we're funding research by academics at Columbia, George Washington and Ohio State universities. This research project will survey citizens in ten countries to find out what kinds of formats, headlines and sources are most effective in correcting COVID-19 vaccine misinformation and whether fact checks that follow these best practices impact willingness to get vaccinated.
- Google's News Initiative also supported Stanford University's [Big Local News](#) and [Pitch Interactive's](#) launch of the [COVID-19 Global Case Mapper](#), which makes it possible for journalists anywhere in the world to embed up-to-date visualizations of the pandemic on their sites for readers.
- Google also launched a global [Journalism Emergency Relief Fund](#) through the Google News Initiative to support small and medium-sized news organizations producing original news for local communities.
- YouTube undertook a number of initiatives to combat vaccine hesitancy that included the April launch of our "[Get Back To What You Love](#)" campaign, which encouraged people to learn the facts about COVID-19 vaccines. The campaign was promoted on YouTube, broadcast TV, radio, paid social media with the goal of reaching 180 million users in the United States last year. YouTube also partnered with [community-based organizations](#) to answer top of mind questions about COVID-19 and COVID-19

vaccines, including Spanish-language content via curated spotlight playlists on YouTube.

Reporting on Social Media Manipulation and Malign Influence Operations

When we find attempts to conduct coordinated influence operations on our platforms anywhere around the world, we swiftly act by removing content from our services and terminating these actors' accounts, in accordance with our policies. In addition, we take steps to prevent possible future attempts by the same actors, and routinely exchange information and share our findings with others in the industry.

We typically see less such violative activity on our services than other platforms, due in large part to the nature of our services. Nevertheless, we recognize the importance of informing policy makers, researchers, journalists, and the public on the nature of the attacks we see across our services, so as to help inform whole-of-society responses to disinformation.

There are well-known trade-offs to engaging in such disclosures. They include the risk of disclosing so much information that we'd enable malicious actors to better circumvent our defenses, or the risk of unwittingly calling more attention to influence operations than their scale or effectiveness would warrant (thus furthering the harms that they may cause). Finally, not every instance of manipulation of our platforms is worth reporting: in many ways, one could think of the spammers that have sought to circumvent our ranking systems since the early days of Google as engaging in platform "*manipulation*" – and while we do report on actions we take against spam in our annual webspam reports, it is a different kind of threat.

Bearing all these considerations in mind, in May 2020, we introduced a new, quarterly bulletin published by Google's Threat Analysis Group, to share information about actions we take against accounts that we attribute to coordinated influence operations (foreign and domestic). Our actions against coordinated influence operations [are published here](#).

* * *

We appreciate the opportunity to detail our efforts in addressing COVID-19 health misinformation and disinformation across our services. Google and YouTube are committed to providing authoritative content in relation to the COVID-19 pandemic, as well as helping provide support to those impacted by the crisis. We will continue to provide information on our response through Google's [Blog](#) and YouTube's [Help Center](#). Finally, our policy white paper, [How Google Fights Disinformation](#), provides additional information on how we tackle the intention spread of misinformation across our platforms more broadly.

As of: July 15, 2022
Received: May 02, 2022
Status: Pending_Post
Tracking
No. 12p-7810-yyrf
Comments
Due: May 02, 2022
Submission
Type: Web

PUBLIC SUBMISSION

Docket: HHS-OASH-2022-0006

Impact of Health Misinformation in the Digital Information Environment in the United States Throughout the COVID-19 Pandemic

Comment On: HHS-OASH-2022-0006-0001

Impact of Health Misinformation in the Digital Information Environment in the United States Throughout the COVID-19 Pandemic

Document: HHS-OASH-2022-0006-DRAFT-0419

Comment on FR Doc # N/A

Submitter Information

Email: rachelgruner@google.com

Organization: Google LLC

General Comment

See attached file

Attachments

Google Response to the Surgeon General's RFI



Dear Vice Admiral Dr. Murthy,

Thank you for the opportunity to respond to your request for information and the chance to share more about our work to address COVID-19 misinformation and improve health outcomes.

At Meta, we're proud to have helped billions of people connect to trusted and credible health information and to services from trusted health partners. This is true for both the conversations that take place on our platforms and messaging apps, as well as Meta's affirmative efforts, such as our [COVID-19 Information Center](#) and [vaccine finder](#), eligibility and profile frame campaigns, health services offered over WhatsApp, social campaigns like "Stay Home, Save Lives", as well as a [host of other efforts](#). Such work can result in measurable improvements to outcomes, including people who [reduced travel for the holidays in 2020 and reducing subsequent COVID19 case counts](#), increases [in reported mask wearing](#), and increases in COVID-19 [vaccination attitudes](#) and [behaviors](#).

With regard to the main topic of your RFI, as we outline in the attached submission, over the past few years we've taken significant steps to reduce misinformation and related content on our platforms, through both a range of policy changes and fundamental product improvements. These include advancements in our automated detection systems, partnerships with health organizations in the United States and around the world, increased investments in third party fact checking, and stronger crackdowns on fake accounts and deceptive behavior, among other measures. We've worked closely with health experts and authorities, including the CDC and the WHO, incorporating their expert guidance and feedback into the products and policies we build.

This work accompanies extensive policies in place that, in addition to reducing the spread of harmful misinformation, are intended to help people share the type of accurate, reliable information that is among the first lines of defense in a public health crisis. Since the earliest days of the pandemic, we've remained dedicated to upholding those policies, while also allowing people to discuss, debate, and share their experiences related to the COVID-19 pandemic.

This latter point is of particular importance. Misinformation is an easy label to apply, but a difficult one to define. And getting it wrong, or applying it with too heavy a hand, has its own negative impact on what people believe or what sources they trust. Indeed, as you note in the initial footnote to your 2021 [Advisory on Building a Healthy Information Environment](#): what counts as misinformation can change over time with new evidence and scientific consensus. We agree, and agree as well that it is important to be careful to avoid conflating controversial or unorthodox claims with misinformation. We've also seen how things like vaccine hesitancy can be driven, not by misinformation, but by real – though outlying – stories and news coverage that

get attention partially as a function of their uniqueness. Solutions to these complex issues require nuance as much as they require humility in the exercise of rules we set.

This is why we agree completely that limiting the spread of health misinformation will require a “whole-of-society” effort. Such an effort requires every part of our media ecosystem — print, radio, TV, email, and social media — to recognize their role and responsibility in achieving these outcomes. While it’s true that online platforms are typically a secondary source of information relative to TV for many people, and Meta itself doesn’t determine what stories the news covers, we believe that online platforms can play a meaningful role in improving access, for the present pandemic and beyond. Online platforms have unique strengths, like global scale and the ability to personalize content and services at low cost. These can be an amplifying force to the people and organizations who make positive health outcomes possible.

Finally, this response represents a continuation of our ongoing mission to address the problem of harmful misinformation and improve health outcomes. While COVID-19 continues to impact people in the United States and around the world, we remain committed to doing our part to help society overcome this pandemic. We are grateful for the chance to be part of this effort and look forward to continuing our work and our collaboration with your office in the future.

Sincerely,

[information withheld b(5)]

[information withheld b(5)]

Head of Health, Meta

Below please find Meta's responses to the questions in the [Impact of Health Misinformation in the Digital Information Environment in the United States Throughout the COVID-19 Pandemic Request for Information](#) (RFI) related to Technology Platforms (RFI Questions 3 through 6).

We share a common goal of improving health outcomes through improved access to health information, support, and services. As you note, accomplishing this will require a whole-of-society approach, beyond just technology platforms alone. Along these lines, in addition to directly answering your questions, we're also including some additional context that we have found helpful for informing our and our partners' approach on these issues, specifically around:

- 1) *What are the primary drivers of health behaviors and outcomes, and what are the relative roles that different parts of the media ecosystem (online and offline) play?* This helps ensure that we collectively have a whole-of-society understanding of the problems and opportunities, and design holistic solutions.
- 2) *What are solutions that work in improving access to health information, support, and services and health outcomes?* This helps us collectively replicate and scale what works more quickly.

We're grateful for your fostering the conversation on these important issues, and we look forward to learning from the other submissions as part of this RFI. A shared and properly contextualized understanding of our role, as well as the challenges and opportunities, helps us work together on a whole-of-society approach to realize the potential of online platforms in improving outcomes over time.

[RFI Q4] What are our COVID-19 misinformation policies and what data do we have on their implementation and effectiveness?

[The goal](#) of our COVID-19 misinformation policy is to reduce harm to people, while also allowing people to discuss, debate and share their opinions, personal experiences, science, and news related to the COVID-19 pandemic.

As we note in the [policy rationale that accompanies the misinformation section of our Community Standards](#), [there is no simple way to approach this problem](#). The world is changing constantly, and what is true one minute may not be true the next, as we have certainly seen over the course of the pandemic. Media platforms have been used to rapidly disseminate newly changed guidance and information, including around mask wearing and airborne transmission. We have also received guidance from health and communication experts that overcoming vaccine hesitancy depends on people being able to ask legitimate questions about vaccine safety and efficacy and getting those questions answered by trusted sources. The Royal Society of the United Kingdom [recently noted](#) that removing some false claims about COVID-19 can exacerbate feelings of distrust with authorities and further marginalize populations – they instead recommend deeper investments in outreach by trusted organizations online as well as fact-checking. So our policy approach to misinformation needs to balance these trade-offs.

At a high-level¹, our policy approach is as follows:

- We remove a specific set of false claims that global health experts have told us contribute to imminent harm. These are what comprise our COVID-19 Misinformation and Harm Content policy. Entities that repeatedly violate these policies are removed from our platform.
- We reduce the distribution of certain types of sensationalist content about vaccines that does not otherwise violate our policies ("Borderline Vaccine Content").
- We work with a global network of [third-party fact checking partners](#) who review and rate content on our apps. When they rate content as false, we reduce its distribution in Feed so fewer people see it and we add warning labels to the content with additional context so people have more information to decide what to read, trust, and share. Pages, groups, accounts, or websites that repeatedly share content rated false by fact-checkers will have some restrictions, including having their distribution reduced. Pages, groups, and websites may also have their ability to monetize and advertise removed, and their ability to register as a news page removed.

The above policies apply to organic content on Facebook and Instagram. What follows below is a more detailed explanation of said policies. Ads policies are stricter and explained later in our response to the question on sales of products and services.

"COVID-19 Misinformation and Harm Content".

Under our [Community Standards](#):

We remove misinformation during public health emergencies when public health authorities conclude that the information is false and likely to directly contribute to the risk of imminent physical harm, including by contributing to the risk of individuals getting or spreading a harmful disease or refusing an associated vaccine.

Since COVID-19 was [declared by the WHO](#) to be a Public Health Emergency of International Concern (PHEIC) in January 2020, we have applied this policy to content containing claims related to COVID-19 that, according to public health authorities, are (a) false, and (b) likely to contribute to imminent physical harm (imminent physical harm examples include: increasing the likelihood of exposure to or transmission of the virus, or having adverse effects on the public health system's ability to cope with the pandemic).

We also take steps to reduce the distribution of content that our systems predict likely violates this COVID-19 misinformation policy, but that has not yet been confirmed to be a violation; if at any point this content is confirmed to violate the policy then it is removed from the platform.

The full list of false information related to COVID-19 that we remove [is available online](#), but some of the claims include:

More details around our approach to misinformation is covered in the [Misinformation section of the Facebook Community Standards](#), the [COVID-19 and Vaccine Policy Updates & Protections](#) section of the Facebook Help Center, the [Instagram Community Guidelines](#), and the Instagram-specific page relevant to [COVID-19 and Vaccine Policy Updates and Protections](#).

- Claims that deny the existence of the COVID-19 disease;
- Claims that downplay the severity of COVID-19;
- Claims about the cause of COVID-19 that are linked to 5G communications technology;
- Claims about COVID-19 transmission and immunity, such as: claims that any group is immune or cannot die from COVID-19 or that a specific activity or treatment results in immunity;
- Guaranteed cures or prevention methods for COVID-19;
- Claims that discourage good health practices, including claims about COVID-19 vaccines that contribute to vaccine rejection; among others.

We also remove content that repeats certain other false health information, primarily about vaccines, that are widely debunked by leading health organizations such as the World Health Organization (WHO) and the Centers for Disease Control and Prevention (CDC).

"Borderline Vaccine Content"

As part of our efforts to improve the quality of health and vaccine content that people encounter during the COVID-19 pandemic, [we reduce the distribution](#) of certain content about vaccines that does not otherwise violate our policies. This is consistent with the advice of independent health experts and echoes the approach we take with [many](#) of our policy areas.

Examples of this type of content include posts which:

1. Are sensationalist or alarmist about vaccines,
2. Disparage people on the basis of their vaccine choices,
3. Promote vaccine refusals or alternatives, or
4. Share stories about adverse events or side effects after vaccination that are presented in a shocking or hyperbolic way.

[As of August 2021](#), we had removed more than 20 million pieces of content from Facebook and Instagram globally for violating our policies on COVID-19-related misinformation. We have removed over [3,000 accounts, pages, and groups for repeatedly violating our rules](#) against spreading COVID-19 and vaccine misinformation. We displayed warnings on more than 190 million pieces of COVID-related content on Facebook that our third-party fact-checking partners rated as false, partly false, altered or missing context, collaborating with 80 fact-checking organizations in more than 60 languages around the world.

[RFI Q3] How widespread is COVID-19 misinformation on our platforms?

Measuring Misinformation and Harm Content prevalence reliably has been challenging relative to other types of content addressed in our Community Standards, given the changing nature of claims across the pandemic, as well as the evolving nature of expert understanding of the facts and information surrounding COVID-19. With graphic violence or hate speech, for instance, our policies specify the speech we prohibit, and even persons who disagree with those policies can follow them. As we've discussed with government officials and public health experts in conversations about misinformation and the reliability of prevalence data, what is true one

minute may not be true the next minute - for example, COVID-19 vaccine effectiveness wasn't a topic at the beginning of the pandemic since vaccines hadn't been developed yet, and words like 'delta' or 'omicron' took on new meanings as the pandemic developed as did their relationship with potential misinformation.

We have been working on improving our measurement systems over the course of the pandemic to both inform our enforcement efforts and allow for more reliable reporting. As a result of this effort, we can estimate that during March of 2022 content related to COVID-19 or vaccines made up about 1 to 2% of the views on Facebook posts in the US. Of the views on content related to COVID-19 or vaccines, we estimate about 0.1% are on content that violates our Misinformation and Harm policies. We know any amount of this content on our platforms is too much - this content is false and harmful, and we aim to remove it as soon as we find it.

Beyond this effort, we also reduce the distribution of content that could discourage vaccination in sensational or misleading ways (for example through exaggerating safety concerns or disparaging those who vaccinate) as part of our efforts to improve the quality of vaccine information on our platforms. During March of 2022, over 95% of all views on US posts related to vaccines on Facebook did not fall into this category (content that could discourage vaccination in sensational or misleading ways).

[RFI Q5] What are the main sources of COVID-19 misinformation?

We have seen Misinformation and Harm and Borderline Vaccine Content come from several sources, including individuals, public officials, and media coverage on vaccine side effects or regulatory approval processes.

It's important to clarify a widely circulated claim that the global problem of COVID-19 vaccine misinformation can be largely solved simply by removing 12 people from social media platforms: specifically, that 12 people are responsible for a large majority of online vaccine information on Facebook. Misconceptions about the problem being predominantly the result of 12 people can distract from finding meaningful and effective solutions to what is a complex problem.

In reality, as of Aug 2021, these 12 people are responsible for about just 0.05% of all views of vaccine-related content on Facebook. This includes all vaccine-related posts they've shared, whether true or false, as well as URLs associated with these people. [The report](#) upon which the claim is based analyzed a narrow set of 483 pieces of content over six weeks from only 30 groups, some of which are as small as 2,500 users. They are not representative of the hundreds of millions of posts that people have shared about COVID-19 vaccines in the past months on Facebook. [More context can be found in this post.](#)

[RFI Q6] What information do we have about COVID-19 misinformation related to the sale of unproven products or services or other money-making models, and what is our approach?

Starting early in the pandemic, we saw some people trying to exploit the pandemic for financial gain. To better protect people from this type of behavior, we put several policies in place related to the sale of certain products as well as how the products could be marketed.

Within the Misinformation and Harm Policy detailed in RFI Q4, we remove certain false claims about how to cure or prevent COVID-19, including those about some unproven products or services. These apply to both organic content and Ads. The claims include:

- Claims that for the average person, something can guarantee prevention from getting COVID-19 or can guarantee recovery from COVID-19 before such a cure or prevention has been approved, including:
 - Consuming or inhaling specific items
 - Medical or herbal remedies
 - External remedies for the outer body or skin
- Ex: “Take Vitamin C - it cures COVID-19,” “If you take this herbal remedy, you will not get COVID-19,” “This topical cream will prevent you from contracting coronavirus.”

On top of these policies, we have additional, stricter policies for ads and commerce surfaces (e.g. Marketplace, Shops). For example, early in the pandemic, when medical supplies were scarce and experts advised a need to conserve them for the healthcare system, we [temporarily banned ads and commerce listings for masks](#). We did this to help protect against scams, medical supply shortages, inflated prices and hoarding. We took down millions of ads and commerce listings in this space during this period. As expert guidance changed and health authorities moved to advise wearing masks, and we saw people and businesses working to fill this need, we scaled back that ban.

We’ve taken similar approaches on other products and services like COVID-19 testing kits. With the initial low supply, we temporarily restricted advertising of these kits on our platforms - in line with government and health authority recommendations - to preserve allocation of these kits to the individuals and regions most in need. As these have become less constrained, we relaxed this restriction, but continue to prohibit misleading claims about tests.

We also continue to prohibit peer-to-peer sales, including peer-to-peer sales on our commerce surfaces, and we require that advertisers be in good standing to advertise these products, with a minimum advertising history of four months.

[Additional Context Q1] What are the primary drivers of health behaviors and outcomes, and what are the relative roles that different parts of the media ecosystem (online and offline) play?

The primary driver of health outcomes is access: to services, support, and information. Within media channels, TV is typically the primary source that people use to obtain information about important issues relative to online or Facebook. According to a [2020 Pew Survey](#), the majority of U.S. adults get their political and civic news from traditional news channels, with 53% getting

it from TV or radio, and 25% from a news website or app. Social media was 18%. Similarly, in a Feb 2021 survey of US FB users, we found that TV was more often reported as the primary source for COVID-19 vaccine information (27%) than Facebook (6%).

Instances of notable changes in vaccination rates due to media over the past few decades have been primarily driven by mainstream coverage, with a disproportionate impact from trusted entities, both positive and negative. For example, Denmark [had a dramatic decline in HPV rates](#) around 2015 after a TV channel broadcast a documentary questioning the safety of the vaccine. Practices such as leading stories with questions and disproportionate coverage of outlier cases can sometimes inadvertently be drivers of hesitancy. Denmark then [saw an increase in HPV vaccination rates](#) after a cross-sector and cross-platform outreach strategy to parents, including on Facebook.

We have also seen how our platform has improved access and outcomes over the course of the pandemic, both via the activity that occurs every day, as well as our affirmative efforts. Evidence here is covered in more detail in the next question, but a few highlights include:

- On information, billions of people have connected to information from trusted health partners via the COVID-19 Information Center, \$100M in ad credits we have given to partners worldwide, and other efforts. Many of these campaigns have been externally validated to drive measurable improvements to outcomes.
- On services, over 3 billion messages have been sent between governments and citizens over COVID-19 vaccine helplines on WhatsApp. In Indonesia, half a million [healthcare workers booked their COVID-19 vaccination](#) directly over WhatsApp in the first 5 days the service was live – this is [1/3 of all healthcare workers in the country](#).

[Additional Context Q2] What are solutions that work in improving access to health information, support, and services and health outcomes?

While online channels are not typically the primary driver of access and outcomes, they do have unique attributes, including global scale and the ability to personalize content and services, at low cost. The unique attributes of online platforms cut both ways (positive and negative).

If properly leveraged, we believe that online platforms can play an increasingly meaningful role in improving access, both for COVID-19 and beyond. Realizing this opportunity will require a whole-of-society approach, both by platforms and by other health and media stakeholders.

Platforms need to both promote trusted and credible information, support and services, as well as reduce misinformation.

On the former, we've invested deeply in working with trusted health partners to connect billions of people to information and services through efforts like our COVID-19 Information Center; vaccine finders, eligibility and profile frame campaigns; and health services offered over WhatsApp. We've distributed over \$100M in ad credits to partners worldwide to promote trusted information and estimate that this has led to over 80 billion impressions. Over 3 billion messages have been sent between governments and citizens over COVID-19 vaccine helplines

on WhatsApp. In Indonesia, half a million [healthcare workers booked their COVID-19 vaccination](#) directly over WhatsApp in the first 5 days the service was live – this is [1/3 of all healthcare workers in the country](#). Experts have seen that friends and family can influence vaccination decisions, so we also developed vaccine profile frames in partnership with UNICEF and HHS in the US, which are live in many countries around the world. In the US, over [60% of Facebook users have seen a profile frame](#).

Moreover, it has been externally validated that these types of efforts can result in measurable improvements to outcomes. This includes increasing people who [reduced travel for the holidays in 2020 and reducing subsequent COVID-19 case counts](#), increases [in reported mask wearing](#), and increases in COVID-19 [vaccination attitudes](#) and [behaviors](#).

On reducing misinformation, beyond the policy and content moderation approaches detailed in response to RFI Q4, some of the most impactful changes we've made are around how our platforms function:

- On WhatsApp, we now limit [the number of times a message can be forwarded](#) to one chat at a time; one such change reduced total messages forwarded globally by 25%.
- On Facebook, we've changed how we rank Health topics in News Feed to reduce how much we weigh engagement signals and have removed certain categories of health content from our recommendations systems entirely. One such change improved how informative and useful users perceived FB to be for COVID-19 content.
- On Facebook and Instagram, we [display a label with a link to the COVID-19 Information Center on all posts about COVID-19](#).

These types of systemic approaches are robust over the long-term since they do not rely on any content moderation and affect all health content vs. just the content we moderate.

We, like many others, have come to realize that it is critical to focus both on reducing misinformation directly and on improving access – these efforts go hand-in-hand. And, while there are understandable debates on how to appropriately moderate misinformation, the opportunities for providing access are comparatively unbounded, with much broader consensus. For these and other reasons, some experts [believe that](#) “more efforts should be devoted to improving acceptance of reliable information, relative to fighting misinformation.”

Realizing this opportunity to improve access and outcomes requires a [whole-of-society](#) approach, beyond what platforms can do alone. Platforms don't create telehealth services, or health information or support, or decide what the media covers or how it is covered – instead, we can be an amplifying force to the people and organizations who do this well. This requires that leaders and organizations invest in meeting the people they serve where they are, online, across all parts of society. In the last 4 years, we've seen tremendous progress here globally and locally, but it has been uneven. These are whole-of-society problems that require whole-of-society solutions.

As of: July 15, 2022
Received: May 02, 2022
Status: Pending_Post
Tracking No.: l2p-7ikt-72zl
Comments
Due: May 02, 2022
Submission Type: Web

PUBLIC SUBMISSION

Docket: HHS-OASH-2022-0006
Impact of Health Misinformation in the Digital Information Environment in the United States Throughout the COVID-19 Pandemic

Comment On: HHS-OASH-2022-0006-0001
Impact of Health Misinformation in the Digital Information Environment in the United States Throughout the COVID-19 Pandemic

Document: HHS-OASH-2022-0006-DRAFT-0420
Comment on FR Doc # N/A

Submitter Information

Email: kxjin@fb.com
Organization: Meta Platforms

General Comment

See attached file(s)

Attachments

- Meta Platforms RFI Submission Cover Letter
- Meta Platforms RFI Submission

DEFENDANTS' EXHIBIT 71:

Taking action to combat COVID-19 vaccine misinformation

At Facebook, we're working to help people get vaccinated by improving access to information about vaccines and how to get vaccinated, making it easier for people to share their support for vaccines, and reducing misinformation about vaccines. While the Surgeon General said "*Limiting the spread of health misinformation is a moral and civic imperative that will require a whole-of-society effort*," we've already taken action on the [eight recommendations from the Surgeon General](#) about what technology platforms can do on COVID-19 misinformation.

1. **Assess the benefits and harms of products and platforms and take responsibility for addressing the harms.** In particular, make meaningful long-term investments to address misinformation, including product changes. Redesign recommendation algorithms to avoid amplifying misinformation, build in "frictions" -- such as suggestions and warnings -- to reduce the sharing of misinformation, and make it easier for users to report misinformation.

We are consistently updating our policies and systems to remove and/or reduce harmful content, including COVID misinformation, not to amplify it. We use a combination of artificial intelligence, human review, and input from partners -- including fact checkers and health organizations -- to address problematic content. We are constantly improving our systems. We review proposed product changes carefully to ensure they have a positive impact.

We have taken numerous steps to ensure people see reliable, high quality content about COVID-19 and how to get vaccinated -- and those efforts are working:

- a. 3.3 million people have visited our vaccine finder tool to get appointment information from a provider's website, get directions to a provider or call a provider about COVID vaccines.
- b. 2 billion people have connected with reliable information about COVID and vaccines through our COVID Info Center
- c. More than 5 million people in the US, and more than 10 million people globally, have used COVID-19 vaccine profile frames to share their support for vaccines. And more than 50% of people in the US on Facebook have already seen someone use the COVID-19 vaccine profile frames, which we developed in collaboration with the US Department of Health and Human Services and Centers for Disease Control and Prevention.

In April 2020, we started showing messages in News Feed to people who liked, commented on or reacted to posts with misinformation about COVID-19 on Facebook that we removed for violating our policy.

We add labels to Facebook and Instagram posts that discuss the COVID-19 vaccines. These labels include reliable information about the safety of COVID-19 vaccines from the World Health Organization. For example, we're adding a label on posts that discuss the safety of COVID-19 vaccines that notes COVID-19 vaccines go through tests for safety and effectiveness before they're approved. We've also added an additional screen when someone goes to share a post on Facebook and Instagram with an informational COVID-19 vaccine label. It provides more information so people have the context they need to make informed decisions about what to share.

Each time a fact-checker rates a piece of COVID-19 content as false, Facebook significantly reduces the content's distribution so that fewer people see it. We notify people who previously shared the content or try to share it that the

information is false, and apply a warning label that links to the fact-checker's article, disproving the claim with original reporting. We also use AI to scale the work of fact-checkers by applying warning labels to duplicates of false claims, and reducing their distribution.

Pages, groups, accounts, or websites that repeatedly share content rated False or Altered by fact-checkers will have some restrictions, including having their distribution reduced. Pages, groups, and websites may also have their ability to monetize and advertise removed, and their ability to register as a news Page removed.

We want to give people more information before they like a Page that has repeatedly shared content that fact-checkers have rated, so you'll see a pop up if you go to like one of these Pages. You can also click to learn more, including that fact-checkers said some posts shared by this Page include false information and a link to more information about our fact-checking program. This will help people make an informed decision about whether they want to follow the Page.

Users can easily report misinformation on any piece of content by clicking on the three dots on the top right corner, clicking "Find support or report post," then "False information."

-
2. **Give researchers access to useful data to properly analyze the spread and impact of misinformation.** Researchers need data on what people see and hear, not just what they engage with, and what content is moderated (e.g., labeled, removed, downranked), including data on automated accounts that spread misinformation. To protect user privacy, data can be anonymized and provided with user consent.

CrowdTangle is a tool from Facebook that makes it easy for academics, journalists, and the public to follow, analyze, and report on what's happening with public content on social media content. People can find larger trends to understand how public content spreads on social media. We have several COVID-19 Live Displays publicly available to see what content is being shared on social media about the virus.

Since April 2020, we've been collaborating with Carnegie Mellon University and University of Maryland on a global survey to gather insights about COVID-19 symptoms, testing, vaccination rates and more. This is the largest survey of its kind, with over 60 million total responses, and more than 170,000 responses daily across more than 200 countries and territories. This effort generates localized insights for researchers, public health officials and policymakers who are working to end the pandemic as quickly as possible.

-
3. **Strengthen the monitoring of misinformation.** Platforms should increase staffing of multilingual content moderation teams and improve the effectiveness of machine learning algorithms in languages other than English since non-English-language misinformation continues to proliferate. Platforms should also address misinformation in live streams, which are more difficult to moderate due to their temporary nature and use of audio and video.

We use experienced teams and technology to find and remove misinformation that breaks our rules on COVID and vaccine misinformation. While we're constantly working to improve our systems, we believe we have some of the strongest systems in place to identify and take action against misinformation that breaks our rules.

In addition, we work with more than 80 global fact-checking partners to review and debunk misinformation, including claims about COVID and vaccines, in more than 60 languages. Since the beginning of the pandemic, we've labeled hundreds of millions of pieces of COVID-19 content rated false by our network of fact checking partners.

We're operating our entire comprehensive strategy to combat COVID-19 misinformation in Spanish. This includes running the largest online vaccine information campaign in history and enforcing our policies and removing false claims about COVID-19 and vaccines - all in Spanish. We use the same machine learning model approaches in Spanish as we do

in English to remove misinformation that violates our Community Standards, and we have four US-based fact-checking partners who review and rate content in Spanish.

-
4. **Prioritize early detection of misinformation “super-spreaders” and repeat offenders.** Impose clear consequences for accounts that repeatedly violate platform policies.
-

We have strong policies to remove false claims about COVID and vaccines that we enforce - and when a Page, Group, or account repeatedly violates these policies we enforce penalties against them, including removing entities that repeatedly break our rules from our platforms.

Pages groups, accounts, or websites that repeatedly share content rated false by fact-checkers will have some restrictions, including having their distribution reduced. Pages, groups, and websites may also have their ability to monetize and advertise removed, and their ability to register as a news Page removed.

5. **Evaluate the effectiveness of internal policies and practices in addressing misinformation and be transparent with findings.** Publish standardized measures of how often users are exposed to misinformation and through what channels, what kinds of misinformation are most prevalent, and what share of misinformation is addressed in a timely manner. Communicate why certain content is flagged, removed, downranked, or left alone. Work to understand potential unintended consequences of content moderation, such as migration of users to less-moderated platforms.
-

We have clear policies in place for what violates our rules on COVID and vaccine misinformation that are publicly posted, including in our [Help Center](#), and we always aim to remove violating content as quickly as possible. We use a combination of people and technology to find and remove this violating content as quickly as possible and we’ve removed millions of pieces of content to date. We’ve also continued to adjust the list of claims that violate our policies to account for changing aspects of the pandemic. For example, we’ve recently added claims around theories that COVID vaccines make you ‘magnetic’ and viral ‘shedding’ that we remove from our apps.

We take a number of steps to identify, review, and remove potential misinfo before it goes viral, including temporary demotions of some content that is awaiting review by our third-party fact-checkers and monitoring the top viral content on our platform.

When COVID-19 misinformation does not present risk of contributing to imminent physical harm but is fact-checked by one of our partners, we label and reduce the visibility of that content. We also add informational labels to content about COVID-19 vaccines while promoting authoritative information on COVID-19 and vaccines. These measures play a key role in promoting understanding about COVID-19 and the COVID vaccine, further reducing the spread of misinformation.

6. **Proactively address information deficits.** An information deficit occurs when there is high public interest in a topic but limited quality information available. Provide information from trusted and credible sources to prevent misconceptions from taking hold.
-

An important component of our strategy to combat COVID-19 misinformation and to inform our community is to develop tools that promote vaccines and connect people to authoritative information from trusted sources:

Making it easier to get vaccinated: We’re providing authoritative information to help people find vaccine appointments in their area through News Feed messages. We’ve heard from states that this has had an impact: West Virginia reported their vaccine registrations increased significantly after we started promoting eligibility information in News Feed. The CDC launched a Spanish-language vaccine finder on WhatsApp, making it easy to find a location to get the shot, order a free ride and get information.

Helping people get questions answered: We've delivered 10B impressions worldwide of ads supporting partner campaigns since January. A single "Facts about COVID19" News Feed campaign increased belief in key facts about vaccine safety and testing by 3% across 5 countries. We've directed 2B+ people to expert health resources through the COVID Information Center.

Social norming through profile frames: We know from public health research that people are more likely to get vaccinated if they see others in their community doing so. Working with the HHS and CDC, earlier this year, we launched profile frames for people to share they've been or are planning to get vaccinated. In the US, more than 50 percent of Facebook users have seen someone they follow use one of these frames in News Feed. Since launch, 5M+ people in the US, including 10M+ people globally, have used these frames; vaccine stickers on IG have been used 7M+ times.

Supporting low vaccination rate communities: We're more frequently reaching people in areas with lower vaccination rates using CDC's Social Vulnerability Index. We are partnering on campaigns with KFF (Kaiser Family Foundation), featuring black doctors, nurses and researchers, and Spanish-language campaigns from Johns Hopkins University's Bloomberg School of Public Health.

Informing vaccination efforts through data: In collaboration with CMU and UMD, we're running the largest global health survey ever conducted, with over 60M total responses to date. This survey is used by Institute for Health Metrics and Evaluation (IHME) and governments around the world. In the US, broad trends are positive since January: vaccine acceptance has trended up overall and racial/ethnic disparities have reduced. We're also offering our Brand Lift measurement platform to help partners replicate and extend approaches that are working.

Trainings for people to spot misinformation: We're partnering with PEN America to offer media literacy training sessions for underserved communities around the US. Their Knowing the News program equips people with skills to evaluate the information they read about COVID-19 and vaccines.

-
7. **Amplify communications from trusted messengers and subject matter experts.** For example, work with health and medical professionals to reach target audiences. Direct users to a broader range of credible sources, including community organizations. It can be particularly helpful to connect people to local trusted leaders who provide accurate information.

Since January 2021, we've given more than \$30 million in ad credits to help governments, NGOs and other organizations reach people with COVID-19 vaccine information and other important messages. These information campaigns resulted in an estimated 10 billion ad impressions globally. We're also adding authoritative information to posts about vaccines on Facebook and Instagram that link to the COVID-19 Information Center for more resources.

We're also providing authoritative information to help people find vaccine appointments in their area through News Feed messages. The CDC launched a Spanish-language vaccine finder on WhatsApp, making it easy to find a location to get the shot, order a free ride and get information.

-
8. **Prioritize protecting health professionals, journalists, and others from online harassment,** including harassment resulting from people believing in misinformation. communications from trusted messengers and subject matter experts.

Any journalist can register with Facebook to get important safety features that protect against harassment, hacking and other unusual account activity, and other issues journalists face online. More details [here](#). In April, we updated our policies to remove coordinated attempts to attack people for their choices around COVID vaccines as we believe this activity constitutes harassment and should be banned from our platforms.

DEFENDANTS' EXHIBIT 72:



Home Policy Analysis Rapid Response
Weekly Briefings

May 4

Rumor Control: a Framework for Countering Vaccine Misinformation

Authors: [Matt Masterson](#), [Alex Zaheer](#), Chase Small, [Jack Cable](#), Jennifer John (Stanford Internet Observatory)

Introduction

There has been a lot of good news recently about the COVID-19 vaccine rollout in the United States. Millions of Americans are [getting vaccinated each day](#), and recent research findings have demonstrated the [long term-effectiveness](#) of the vaccines. However, as the United States begins to approach what appears to be a plateau in vaccination rates, we will likely see a transition in the type and pervasiveness of mis- and disinformation about the safety, availability and effectiveness of the COVID-19 vaccines. Those who want the vaccine have largely gotten it, and many of the adults who remain are either hesitant or have difficulty getting access to the vaccine. Trials for children have also begun, with the [FDA set to authorize](#) the first vaccine for adolescents imminently. As issues of access are addressed, lingering vaccine hesitancy has the potential to delay the long-awaited end to the pandemic, so understanding persistent vaccine hesitancy is key. [Many of the narratives underpinning vaccine hesitancy are predictable](#) – they are themes and messaging borrowed from prior efforts to promote hesitancy in other vaccines, including routine childhood immunizations. The key question: who should address them, and how?

What is Rumor Control?

In the context of countering misinformation, a Rumor Control page is a centralized website offered by a trusted voice sharing facts and information in order to anticipate and respond to emerging narratives. This approach to debunking misinformation draws on [literature suggesting](#) that debunking messages coming from rumor control centers can help prevent rumor spread. Psychologists [have concluded](#) that messengers that are perceived as having high trustworthiness and expertise are most effective at debunking falsehoods, meaning a debunking approach that aggregates facts from trusted subject matter experts could be ideal. Additionally, in the vaccine context, a study [suggests](#) that trustworthy sources of information highlighting expert consensus around known vaccine-related facts and findings can increase general support for vaccines. A Rumor Control site should never be viewed as the only source of truth, but instead, as a distribution channel to drive visitors to additional information about a complicated subject. Operators must recognize that Rumor Control sites should not address all false or misleading narratives: instead, they should address those that are either anticipated to gain widespread traction or have already received such attention on social or traditional media.

In order to respond to shifting narratives promoting vaccine hesitancy, the operators of a Rumor Control site should identify clear processes for both formulating responses to rumors and consulting subject matter experts. When leveraged effectively, these sites serve as a force multiplier for trusted information sources, enabling other trusted voices to leverage an established Rumor Control site towards tailoring communications for their own communities. Federal, state and local health officials and healthcare providers have begun a version of this by [providing reassurance and](#) correcting misconceptions as vaccine distribution continues, but the effort remains disjointed [compared to](#) the highly-networked and coordinated anti-vaccine community. For inspiration on how to better connect the “defenders” here, we look at another recent event that involved a flood of false and misleading information: the 2020 election.

Rumor Control and the 2020 Election

The Rumor Control established during the U.S. 2020 election by the Cybersecurity and Infrastructure Security Agency (CISA) serves as a case study for the potential impact and usage of such a site. In the lead-up to this election, all levels of government and the major social media platforms collaborated to anticipate and debunk election-related narratives. For example, as states made changes to the election process due to COVID-19 restrictions, election officials used both social and traditional media to reach out to voters directly regarding when and how to return mail ballots, or explaining why [election results would take longer to report due to these mail-in ballots](#).

As local officials launched their individual Rumor Controls across the country, CISA, the lead federal agency for election security, recognized a need to address larger delegitimizing themes at a national level. As narratives or questions emerged, state and local officials used Rumor Control pages as hubs to share facts and official messaging to voters. This need was highlighted when Iranian actors launched a disinformation campaign that threatened voters with consequences based on their voting preferences. Thus, the CISA Rumor Control page was born, to anticipate and debunk emerging rumors at a national level before they went viral. CISA's Rumor Control ultimately rose to national attention for championing the role of state and local election officials in securing the election, and today, is regarded by election officials as one of the most effective efforts toward countering mis- and disinformation in the 2020 election.

While election-related and vaccine-related misinformation differ in content, efforts to counter one may inform efforts to counter the other, particularly related to synchronization of public messaging. Similar to election communications, public health communication relies on a network of actors at many levels of locality and across various communities. This makes message coordination among all public health communicators elusive, a daunting fact given the pervasiveness and spread of vaccine mis- and disinformation seen to date. In the 2020 election, CISA's Rumor Control page emboldened state and local election officials to create their own information hubs, often using CISA's example as a template. Similarly, in the vaccine space, a Rumor Control operator could work to identify pervasive narratives at a local or national level, then collect facts accordingly from subject matter experts to debunk these narratives and mobilize this process into an operational Rumor Control.

Operating Rumor Control: a Framework

Rumor Control Workflow

Rumor Control efforts should follow pre-established workflows to ensure that only relevant myths are addressed, proper subject matter experts are consulted in drafting the myth-debunking, and all relevant communicators amplify the fact after publication to reach its intended audience. While an initial version of these procedures should be determined before the Rumor Control is created, as public perception of this page is observed and analyzed, communicators should iterate and make adjustments.

Figure 1: Proposed Rumor Control Workflow

Figure 1 shows a potential Rumor Control workflow, which is outlined in more detail below:

1. **Myth Detected:** The Rumor Control operator receives reports from community partners such as doctors, vaccine administrators, community-specific liaisons, or through internal detection and monitoring to determine which narratives are gaining traction in key communities.
2. **Response Threshold Triggered:** The Rumor Control team continually monitors the spread of the myth online, regularly evaluating whether or not the thresholds for response have been met.
3. **Fact Drafted and Published:** Once the threshold has been met, the Rumor Control operator consults with subject matter experts to determine ground truth and the best way to debunk the observed myth, and publishes the result.
4. **Fact Amplified:** The Rumor Control operator engages with community partners to amplify the accurate information through whichever communication channels best reach the target communities. Given that falsehoods may spread further and faster than facts on social media, this step is critical to ensuring factual information receives as much reach as possible in the appropriate online communities.
5. **Reaction Measured:** After the Rumor Control posting is disseminated widely, the operator checks in with community partners and other stakeholders to determine the continued pervasiveness of the debunked myth. While discerning the causal impact of the Rumor Control posting is not easy, this process will yield valuable feedback on the current Rumor Control workflow and identify opportunities for improvement, such as whether thresholds for response should be lowered to future rumors on a certain topic given past spread.

Strong partnerships with community-specific subject matter experts and liaisons are critical to this workflow. Partners can include state and local government offices, civil society members, NGOs, and individual organizers. Not only should these individuals help in sourcing and assessing the impact of pervasive narratives, but they will also be the core amplifiers of Rumor Control postings to each target audiences. Building these partner relationships takes time, and should be started as early as possible in the Rumor Control development process.

Effectively Presenting Facts

An effective Rumor Control page addresses rumors directly and uses language that is accessible to the general public. Each rumor explanation should follow the same format: a factual statement, followed by a single sentence summarizing the rumor, and finally a deeper factual debunking of the rumor.

- Start with the facts. Research shows that overall, debunking misinformation does decrease belief in the targeted falsehoods. The most effective debunking strategy is presenting factual information about the topic in question. Draft Rumor Control posts with this in mind, sourcing your facts from trustworthy subject matter experts such as local doctors, hospital associations or health offices
- Write in plain, accessible language. Especially in a social media environment, factual information used to debunk falsehoods are ideally accessible to the average layperson. Statements should be succinct and visually appealing. Posts to social media promoting Rumor Control should include images and diagrams if those are available.
- Link to other trusted sources, not the rumor itself. Avoid linking to instances of the original myth. Instead, link to authoritative sources on the subject that are likely to be widely recognized as independent and trustworthy.

Example Rumor Control Format

Reality: COVID-19 vaccines do not change or interact with your DNA in any way.

Myth: COVID-19 vaccines are designed to change your DNA

Get the facts: There are currently two types of COVID-19 vaccines that have been authorized and recommended for use in the United States: messenger RNA (mRNA) vaccines and a viral vector vaccine. All COVID-19 vaccines work with the body's natural defenses to safely develop immunity to disease. The vaccines never enter the nucleus of the cell, which is where our DNA is kept. This means the genetic material in the vaccines cannot affect or interact with our DNA in any way. For more information, see the [CDC's explanation of mRNA vaccines](#).

Adapted from <https://www.cdc.gov/coronavirus/2019-ncov/vaccines/facts.html>

Recommended Thresholds for Posting to Rumor Control

Operators of a Rumor Control site should only address topics that the average reader will have already heard about, or is likely to encounter. [First Draft, a non-profit organization that works with journalists, academics, technologists on how to provide accurate information in critical moments, highlights five criteria to consider](#) when determining when to report on misinformation. Below, we have placed these thresholds in the context of a Rumor Control website:

Engagement – Rumor Control websites should address misinformation that has received a high level of attention across multiple posts. Operators can search keywords of a rumor on Google, Facebook, or Twitter to assess if it appears in multiple posts with a high cumulative number of engagements. For example, it would not be appropriate to address a false claim made by an individual online that has only been liked a handful of times, as doing so would likely expose people to the rumor who otherwise would never have encountered it. Data & Society have provided [guidelines](#) on the danger of amplification when communicating about harmful content.

Audience – While online anti-vaccine communities and accounts post vaccine misinformation incessantly, Rumor control sites should only address a rumor found in these groups if it has spread to the general public. Operators should look for instances where an online group that rarely talks about vaccines discusses an anti-vaccine narrative. For instance, when a narrative moves beyond anti-vaccine groups, to political forums or parenting groups, this is indicative of more general spread.

Multiple Social Media Platforms – Rumor Control websites should consider whether misinformation has spread across multiple social media platforms. To identify additional content, key terms and URLs associated with the initial post will be searched for across different platforms. Content that has spread across multiple major platforms and met other criteria above has likely gained enough traction to warrant a Rumor Control post.

Influencer/Verified Accounts – Rumor Control websites should address misinformation that has been amplified by verified accounts and other influencers who may have a large and active following that is likely to amplify their message. If the influencer does not generally discuss vaccines, the narrative is likely to pose a greater threat.

Large Media Outlets – Rumor Control websites should address misinformation that has been amplified by large media outlets like cable news or online newspapers. Even if the media outlets are debunking and countering the misinformation, it will be important to include in the Rumor Control site.

When in doubt, Rumor control sites should seek the support of mis- and disinformation researchers to assess the pervasiveness of rumors. Research institutions such as those that make up the [Virality Project](#), [FirstDraft](#), and [Project VCTR](#) can be helpful for determining if a rumor meets the above criteria.

As vaccination rates in adults plateau and child vaccinations begin, misleading information about vaccines will likely intensify, and therefore so should efforts to counteract it. The Rumor Control model offers an opportunity to use networked influencers — a tactic employed heavily by disinformers — across sectors to amplify facts over rumors. If it is successful in the vaccine space, this could be an important tool in demonstrating that a truly “whole-of-society” response to harmful mis- and disinformation is possible.

< The Case for a Mis- and
Disinformation Center of
Excellence

Vaccine Rollout and
Mis/Disinformation:
Expectations and Action Plan
for Health Communicators

>

DEFENDANTS' EXHIBIT 73:



Home Policy Analysis Rapid Response
Weekly Briefings

Feb 11

Announcing the Virality Project

Anti-vaccine disinformation will pose significant challenges to the rollout and public adoption of COVID-19 vaccines in the United States. The anti-vaccine movement has well-developed online networks and expertise in leveraging social channels to spread its messages. These networked activism efforts have linked longtime anti-vaccine activists, health and wellness influencers, those who object to vaccination requirements as government overreach, and politically-driven communities who have actively amplified COVID and other conspiracies. The movement is experienced, well-funded, and able to generate in-the-streets action. It has already begun to expend significant efforts to enter mainstream conversation and erode confidence in COVID-19 vaccines.

The **Virality Project** is a coalition of research entities focused on supporting real-time information exchange between the disinformation research community, public health officials, civil society organizations, government agencies, and social media platforms. Our objective is to detect, analyze, and respond to incidents of false and misleading narratives related to COVID-19 vaccines across online ecosystems, enabling civil society and health communicators to ultimately mitigate the impact of narratives which might otherwise undermine the public's confidence in the safety of evidence-based policies in the United States.

The Partnership consists of analysts across six of the nation's leading institutions focused on analysis of mis- and disinformation in the social media landscape: the [Stanford Internet Observatory](#), the [University of Washington's Center for an Informed Public](#), [New York University's Center for Social Media and Politics](#) and [Tandon School of Engineering](#), [Graphika](#), and the [National Conference on Citizenship](#). Members of this coalition bring with them the insights gained from their previous collaboration on the [Election Integrity Partnership](#) which, during the 2020 Election, coordinated the work of 120 analysts,

published 32 blogposts on findings, and worked directly with platform partners to respond to over 800 unique incidents of election-related disinformation.

In the coming weeks, we expect to add more institutions as core research collaborators. We look forward to a full launch webinar involving all of these organizations at that point.

The Virality Project will provide actionable situational awareness and response capabilities for public health officials and other partners on the front lines of providing accurate vaccine-related information to the public. *Public officials, civil society, and health sector organizations can reach the team at info@viralityproject.org.*

DEFENDANTS' EXHIBIT 74:

Background on the SIO's Projects on Social Media

 cyber f i tanford edu/io/new /background io project ocial media

Breadcrumb

1. [All Internet Observatory News](#)
2. News
3. March 17, 2023

Stanford Internet Observatory

Various inaccurate and misleading claims have been made in the media and in congressional testimony regarding the Stanford Internet Observatory's projects to analyze rumors and narratives on social media relating to U.S. elections and the coronavirus. As explained in the [statement](#) issued by our partners at the University of Washington, it is difficult to rebut all of these inaccurate claims without repeating the falsehoods and contributing to their further spread. Nevertheless, the SIO believes it is important to respond to inaccurate statements about its work and to correct the public record. This fact sheet provides background on the SIO's activities and corrects a number of false allegations.

1. The [Stanford Internet Observatory](#), founded in June 2019, is a non-partisan, cross-disciplinary program of research, teaching and policy engagement for the study of abuse in current information technologies, focusing on social media. The SIO studies and publishes about disinformation and state influence operations and conducts and publishes research regarding child internet safety, online platforms' policies and practices toward self-harm, and privacy-protecting technologies.
2. The SIO is one of four organizations that convened the [Election Integrity Partnership](#) (EIP) and [Virality Project](#) (VP). The EIP and VP, both founded in 2020, are non-partisan research coalitions that operate in an open, transparent, and public manner, publishing [blog posts](#), [weekly updates](#), [briefing videos](#), [academic papers](#), and voluminous [investigative reports](#) relating to election and vaccine misinformation, disinformation, and propaganda.
3. The EIP's goal was and continues to be to research and analyze attempts to prevent or deter people from voting, as well as efforts to delegitimize election results. The EIP did not study online discussions of specific candidates, parties, or political topics in the 2020 or 2022 election cycles. The EIP did not make recommendations to social media or take any other actions regarding content about the Hunter Biden laptop story.

4. The VP was established to research viral narratives on social media related to COVID vaccines in four areas “(1) safety, (2) efficacy and necessity, (3) development and distribution, and (4) conspiracy theory[.]” Its primary goal was to facilitate awareness for public health officials and medical professionals seeking to communicate accurate information to the public
5. The EIP and VP provided public factual findings to multiple entities, including government agencies and social media platforms, but had no control over content moderation, censorship, or labeling posts. Emails released in the Twitter Files demonstrate that Twitter’s staff examined any reports sent to them to see if the content was violative of their policies and took no action in cases where they felt that Twitter’s existing policies were not violated.

Was Stanford Internet Observatory’s Election Integrity Partnership created in response to public criticism of DHS’s “Disinformation Governance Board” and to substitute for the work of the government?

No. The EIP was created in the summer of 2020, long before the announcement and media criticism of the Disinformation Governance Board in April 2022.

Does the SIO or EIP receive funding from the federal government?

As part of Stanford University, the SIO receives gift and grant funding to support its work. In 2021, the SIO received a five-year grant from the National Science Foundation, an independent government agency, awarding a total of \$748,437 over a five-year period to support research into the spread of misinformation on the internet during real-time events. SIO applied for and received the grant after the 2020 election. None of the NSF funds, or any other government funding, was used to study the 2020 election or to support the Virality Project. The NSF is the SIO’s sole source of government funding.

Is it true that the EIP censored 22 million tweets and labeled them as “misinformation”?

No, the EIP did not censor any tweets or label any tweets as “misinformation.” EIP has no ability to remove or label tweets or other posts, and content moderation decisions are independently made by social media platforms. As part of its non-partisan research relating to the 2020 U.S. presidential election, EIP analyzed 22 million tweets that contained keywords or URLs relevant to EIP’s scope of work. EIP identified 2,890 unique tweet URLs in potential violation of Twitter’s stated policies. EIP provided its factual analysis to the relevant platforms, which were then responsible for each platform’s own content moderation decisions. The EIP informed Twitter and other social media platforms when certain social media posts violated each platform’s own policies; EIP did not make recommendations to the platforms about what actions they should take.

Did the EIP “target” or discriminate against conservative social media accounts or content or seek to promote liberal accounts or content?

No. EIP is a non-partisan coalition dedicated to the identification and analysis of online content that suppresses voting, reduces participation, confuses voters about election processes, or delegitimizes election results without evidence. Based on an analysis of an expansive dataset and without targeting any specific accounts of politically affiliated content, EIP’s research determined that accounts that supported President Trump’s inaccurate assertions around the election included more false statements than other accounts. Through the same analysis, EIP also found and published or flagged examples of false statements and rumors made by accounts linked to left leaning groups and foreign actors. EIP informed social media platforms of examples of violative content by progressive groups as well as conservative groups.

Did EIP receive direct requests from the Department of Homeland Security’s Cybersecurity and Infrastructure Security Agency (CISA) to eliminate or censor tweets?

No. In its non-partisan research during the 2020 and 2022 elections, EIP analyzed reports of potentially false information received from a broad array of sources, including state and local election officials. These reports were channeled through the Election Infrastructure Information Sharing & Analysis Center (EI-ISAC). The EI-ISAC did not ask the EIP to censor or eliminate social media posts. EIP’s role was limited to the analysis of potentially inaccurate information that had been reported to EI-ISAC by state and local election officials. As noted above, the EIP had no ability to censor or eliminate social media posts; it simply identified potentially policy-violative posts to social media platforms.

Did the SIO’s Virality Project censor social media content regarding coronavirus vaccine side-effects?

No. The VP did not censor or ask social media platforms to remove any social media content regarding coronavirus vaccine side effects. Theories stating otherwise are inaccurate and based on distortions of email exchanges in the Twitter Files. The Project’s engagement with government agencies at the local, state, or federal level consisted of factual briefings about commentary about the vaccine circulating on social media.

The VP’s work centered on identification and analysis of social media commentary relating to the COVID 19 vaccine, including emerging rumors about the vaccine where the truth of the issue discussed could not yet be determined. The VP provided public information about observed social media trends that could be used by social media platforms and public health communicators to inform their responses and further public dialogue. Rather than attempting to censor speech, the VP’s goal was to share its analysis of social media trends so that social media platforms and public health officials were prepared to respond to widely shared

narratives. In its work, the Project identified several categories of allegations on Twitter relating to coronavirus vaccines, and asked platforms, including Twitter, which categories were of interest to them. Decisions to remove or flag tweets were made by Twitter.

More information regarding the VP's research regarding vaccine-related narratives and engagement with social media platforms and the government is available through the VP weekly briefings, which were posted publicly throughout the Project, and in the VP's final report

All Internet Observatory News

DEFENDANTS' EXHIBIT 75:



Virality Project Weekly Briefing #32

July 27, 2021 - August 3, 2021

This report was created by analysts from the [Virality Project](#), a coalition of research entities focused on real-time detection, analysis, and response to COVID-19 anti-vaccine mis- and disinformation. The Virality Project supports information exchange between public health officials, government, and social media platforms through weekly briefings and real-time incident response.

Please note that this is our last official briefing. Our analysts will be continuing internal monitoring and sending out newsletters and blog posts with some of our analysis.

In this briefing:

Events This Week	<ul style="list-style-type: none">• Online discussion of breakthrough cases and vaccine efficacy confounds and worries the public• Media coverage lacking accompanying health guidance leaves room for anti-vaccine influencers to use leaked CDC internal slides to undermine confidence in vaccine efficacy.• Gab CEO Andrew Torba claims military members are being forced to take the vaccine or court-martial• Leaked Pfizer contract prompts decontextualized claims regarding Ivermectin and vaccine injury
Ongoing Themes and Tactics	<ul style="list-style-type: none">• A small number of NFL players opposing vaccines are driving online debates about vaccine mandates among sports fans and right wing accounts• Key Statistics• Appendix

Key Takeaways

- Online discussion heavily featured [confusion around the Delta variant, the efficacy of vaccines against it, and popular breakthrough case stories](#).
- Internal document leaks – from both the [Centers for Disease Control](#) and [Pfizer](#) – were once again manipulated to suggest the government is involved in cover-ups around vaccine development, efficacy, and distribution.
- Military officials weighed imposing a COVID-19 vaccine mandate after President Biden ordered the forces to [begin developing a plan to make the vaccine mandatory](#). In response, the CEO of the alt-social media platform Gab, Andrew Torba, spread [misinformation-laden documents for vaccine exemption](#).

Events this week:

Key events from this past week as identified by our analysts and stakeholder partners.

Online discussion of breakthrough cases and vaccine efficacy confounds and worries the public

- Reports of vaccinated people contracting the virus, including a [widely-reported outbreak](#) in Provincetown, Massachusetts, **have helped aid the rise of an anti-vaccine narrative that breakthrough cases mean the vaccine is not working, which is *not true*.**
- Mainstream coverage of superspreader events and stories of [celebrities contracting](#) or [spreading the virus](#) despite full vaccination have gotten attention. These are often pro-vaccine stories that urge additional caution because of the high infectiousness of the Delta variant.
- Major anti-vaccine influencers, including Earthly and [Joseph Mercola](#), have used the opportunity to shed doubt on vaccine efficacy.
 - Mercola implied that breakthrough cases are actually “vaccine failures,” and that health communicators are using the term “breakthrough case” to prop up COVID-19 vaccines and pharmaceutical companies’ reputations.
 - Mercola’s posts regularly go viral; this one likewise received high traction, with a collective 4K interactions on Facebook and Twitter.
- With new information coming out regularly about the Delta variant’s effect on vaccine efficacy, different studies and news outlets have chosen to emphasize different numbers about efficacy: some efficacy rates show symptomatic infection, others show hospitalization, and others show severe illness. The overall “efficacy” of a vaccine can thus be confusing to the public.
 - [Anti-vaccine accounts](#) have picked up these varying numbers to highlight the ones that look the worst, using them to prove the vaccines are not effective whatsoever or not worth getting.
- In at least one conspiratorial Chinese-language Telegram channel that has repeatedly spread anti-vaccine content, users attacked Dr. Fauci and the CDC’s updated mask guidance, claiming that the Delta variant is a “fictional” ploy to mandate vaccines. The post was seen by at least 5.4K users.
- **Key Takeaway:** Breakthrough cases are happening, and they are of serious concern. Though they represent an important reason to get the vaccine, anti-vaccine activists use the term to suggest the opposite: that the vaccine is ineffective and that major public health institutions are deceiving the public about it. **Public health communication must include clear statistics and guidance around the Delta variant, its level of infectiousness, and rates of breakthrough cases broken down by symptoms, illness, and hospitalization.**

Media coverage lacking accompanying health guidance leaves room for anti-vaccine influencers to use leaked CDC internal slides to undermine confidence in vaccine efficacy.

- On July 29, internal slides from a CDC meeting, which were obtained by NBC and first published by [The Washington Post](#), contain still-unpublished data that reveals vaccinated people who



contract COVID-19 may have a similar viral load compared to unvaccinated people who contract the virus. The slides give a [justification](#) for the agency's change in [mask guidance](#) last week. **The agency now recommends unvaccinated and vaccinated people wear masks indoors in areas with high transmission rates.**

- The data has been reported within both mainstream and alt-social media platforms. On the alt-right platform Gab, some users have suggested that the COVID-19 vaccine itself spreads COVID-19.
- This has also gotten attention on anti-vaccine and right-leaning conspiratorial Telegram channels in Spanish. Their posts reached at least 100K users.
- Anti-vaccine channels and publications are using this data to undermine confidence in the efficacy of COVID-19 vaccines by **leaving out important context that vaccinated individuals still have a [much lower likelihood of getting infected](#)**. Right-leaning Facebook accounts reshared a screenshot of a [USA Today article](#) that leaves out the same important context.
 - The screenshots also circulated on Instagram, where two posts re-sharing them amassed over 20K engagements.
- **Key Takeaway: Leaked public health information lacks trustworthy accompanying health messaging, and mainstream media reporting on the leaked information can likewise fail to include crucial guidance.** Anti-vaccine accounts can then more easily characterize the information as evidence that COVID-19 vaccines do not work.

Gab CEO Andrew Torba claims military members are being forced to take the vaccine or face court-martial

- The posts come at a sensitive time for the military's vaccination plan. [Military leaders are racing to vaccinate troops without issuing an order](#), while the [White House called on the Defense Department](#) to look into "how and when" it might mandate a vaccine for military members.
- [Torba's post](#) claims he is "getting flooded" with text messages from military service members who are being forced to take the COVID-19 vaccine or else face court-martial as a consequence of their refusal.
- The main post has amassed around 10K engagements, which is very high for the platform. Subsequent posts containing screenshots of text messages also have engagement in the thousands.
- Torba also wrote a post on [Gab's news site](#) with **links to a variety of documents to help service members request vaccine exemptions on religious grounds**, citing the use of aborted fetal cell lines in the development of the "experimental" vaccines – an old, common anti-vaccine [talking point](#).
 - The documents include misinformation about the vaccines.
 - This post garnered around 10K interactions on Facebook.
 - The documents are being shared in the [QAnon community](#).
- **Key Takeaway:** Torba uses his position to combine anti-mandate rhetoric with vaccine misinformation for a large and dedicated audience. His posts are especially significant given the mainstream media's concurrent coverage of the unfolding debate and announcements about a potential vaccine mandate within the military.

Leaked Pfizer contract prompts decontextualized claims regarding Ivermectin and vaccine injury

- Excerpts from a Pfizer purchasing agreement were leaked via a [viral tweet](#) “exposing” the company. Posts were often accompanied by the hashtag #PfizerLeaks.
- The documents appear to have been originally shared by [Ehden Biber](#), who allegedly obtained the document from the Albanian government. It is unclear how the documents were obtained. The original thread was removed, although a [URL](#) of an archived version of the thread has also circulated among anti-vaccine accounts.
- Joseph Mercola shared the excerpts in two tweets that emphasized two parts of the contract: the company’s [indemnification from harm](#) and that [long-term efficacy and adverse effects](#) of the vaccine are unknown. The tweets received over 3K engagements, with most comments discussing that the vaccines should not be mandated.
- **Key Takeaway:** Vaccine purchasing agreements, including price per dose, have long been the subject of anti-vaccine scrutiny. This leak, though new, does not represent a major shift in discourse.

Ongoing Themes and Tactics:

Ongoing themes and tactics that we track each week including notable vaccine injury stories and overall key statistics about online vaccine discussions.

A small number of NFL players opposing vaccines are driving online debates about vaccine mandates among sports fans and right wing accounts

- The Virality Project has [repeatedly reported on stories of professional athletes](#), particularly Cole Beasley of the NFL, whose reluctance to get vaccinated has sparked online conversation.
- This week, [tweets from Arizona Cardinals wide receiver DeAndre Hopkins](#) and the announcement of the [Minnesota Vikings assistant coach stepping down due to vaccine requirements](#) both received significant attention online.
- Facebook posts about the NFL’s vaccine policies have received over 767K engagements in the past week.
- Online debate over vaccine mandates is mainly political in nature, and often emphasizes vaccination as a personal choice. Professional athletes have contributed to this culture by remaining secretive about their vaccination disclosure.
- This debate also can **provide a platform for misleading or false information about COVID-19 vaccines, including vaccine safety.**
 - Hopkins tweeted that his girlfriend’s brother [experienced heart problems](#) after receiving a vaccine.
- **Key Takeaway:** The ongoing amplification of news around athletes refusing to be vaccinated contributes to the framing of vaccination as a political issue rather than a health issue, ultimately giving way to more online space for vaccine safety misinformation and debates about “medical freedom.”


Key Statistics

Here we contextualize the above narratives by examining the engagement of other posts from this week.

- The top COVID-19 related English-language **Facebook post** containing the word “vaccine” this week is by UNICEF, celebrating vaccinations in Haiti made possible by U.S. donations. The post received 438K interactions (422K reactions, 10.5K replies and 5.3K shares).
- This week’s top **Instagram post** containing the word “vaccine” is by pop star Ariana Grande, encouraging her followers to get the vaccine to protect themselves against the Delta variant, and sharing links to medical resources. The post received 4.48M likes.
- This week’s top **post** with the word “vaccine” on **Reddit** shares an article by NBC retelling the story of a 39 year-old father who died of COVID-19 and reportedly regretted not getting the vaccine. The post received 75.9K upvotes.
- This week’s top **post** from a **recurring anti-vax influencer on Facebook** is by Joseph Mercola, D.O., advertising his book untitled “The Truth About COVID-19.” The post received 1.3K interactions (847K reactions, 316 comments and 87 shares).
- This week’s top **tweet** from a **recurring anti-vax influencer on Twitter** is by Dr. Simone Gold, founder of America’s Frontline Doctors (AFLDS), who called on her followers to boycott fast food chain Shake Shack after its founder Danny Meyer announced they would require proof of vaccination for employees and indoor diners. The tweet received 31K interactions (1.5K replies, 7.1K retweets and 22.3K likes).

Appendix

We have included some notable screenshots from the above incidents. More screenshots and assets can be made available, upon request and as needed!

Links	Screenshot
Example Facebook post that uses NBC News reporting about vaccinated people spreading the virus.	

Joseph Mercola's viral Facebook post calling breakthrough cases "vaccine failures"



Dr. Joseph Mercola ✓
July 21 at 4:08 PM · 🌐

I am old enough to remember when 'breakthrough cases' were called 'vaccine failures'.



PUBMED.NCBI.NLM.NIH.GOV

Primary vaccine failure to routine vaccines: Why and what to do? - PubMed

Visit the COVID-19 Information Center for vaccine resources.
[Get Vaccine Info](#)

1.8K 114 Comments 245 Shares

Tweet about a breakthrough case that includes information about heart problems



Deandre Hopkins ✓
@DeAndreHopkins

Follow

... [@jalenramsey](#) My girlfriend brother in the military got the vaccine and had heart problems right after. When you stand for something they hate you!

Jalen Ramsey ✓ @jalenramsey
I know 2 people right now who got the vaccine but are covid positive.. 🤔 I'm just saying. I wouldn't look at a teammate as bad if he don't get the vax, no pressure from [twitter.com/quincy_avery/s...](#)

1:24 PM - 22 Jul 2021

1,378 Retweets 6,930 Likes

1.0K 1.4K 6.9K

LeVon.Wild 🇺🇸 @Kszn_wild · 1h
Replying to @DeAndreHopkins @jalenramsey
Adams better

2

DEFENDANTS' EXHIBIT 76:



Virality Project @ViralityProject · Feb 17, 2022

...

17 Join us next Thursday, February 24 at 11am PT /2pm ET for the launch of the Virality Project final report along with special guest [@DoctorYasmin](#) and researchers [@noUpside](#) [@cameronhickey](#) [@ChaseSmall5](#) and more.

Register [▶ stanford.zoom.us/webinar/regist...](#)



Thread

14

7



Virality Project
@ViralityProject

...

Livestream:



youtube.com

Narratives and Policies that Shape COVID-19 Vaccine Con...
The Stanford Internet Observatory will host analysts from the Virality Project to discuss the project's findings from a ...

2:08 PM · Feb 24, 2022

1 Like



Don't miss what's happening

People on Twitter are the first to know.

Log in

Sign up



Don't miss what's happening
People on Twitter are the first to know.

Log in

Sign up

DEFENDANTS' EXHIBIT 77:

About CDC



CDC 24/7

Saving Lives, Protecting People™

CDC is the nation's leading science-based, data-driven, service organization that protects the public's health. For more than 70 years, we've put science into action to help children stay healthy so they can grow and learn; to help families, businesses, and communities fight disease and stay strong; and to protect the public's health.

[CDC Mission and Vision](#)

[CDC Moving Forward](#)

Learn More About CDC

[Organization](#) >

[Leadership](#) >

[Funding & Grants](#) >

[History](#) >

CDC Strategic Plan 2022-2027

Advancing Science and Health Equity



COVID-19 Response

On January 21, 2020 CDC launched its agency wide response to the COVID-19 pandemic. It has been the largest response to any disease outbreak in CDC's history.



Preparing & Responding

Our job is to prevent, detect, and respond to diseases wherever they are so that diseases don't come into the United States.



Eliminating Disease

CDC provides domestic and international leadership, as well as laboratory and epidemiology expertise, to respond and work toward eliminating every disease we can.



Ending Epidemics

When epidemics like seasonal influenza, new HIV infections, and opioid overdoses occur, we work to quickly detect and address them to reduce their potential impact in America.

Who We Are

CDC is one of the major operating components of the Department of Health and Human Services



STEM at CDC

STEM offerings for students, teachers, and professionals.



CDC Careers

Learn more about job openings, trainings, or fellowship opportunities.



CDC Museum

Visit the David J. Sencer CDC Museum and learn more about CDC's rich heritage.



CDC Speakers Bureau

The CDC Speakers Bureau has been in existence since August 1998.

Meet the Director

Rochelle P. Walensky, MD, MPH

Rochelle P. Walensky, MD, MPH, is the 19th Director of the Centers of Disease Control and Prevention and the ninth Administrator of the Agency for Toxic Substances and Disease Registry.



[Learn More about CDC Director](#)

[Submit a Speaker Request](#)

Contact Us

Call: 800-232-4636 (800-CDC-INFO)

Email: [CDC-INFO Contact Form](#)

1600 Clifton Road Atlanta, GA
30329-4027 USA

Media Newsroom

Get the latest news and updates
on CDC.

CDC-INFO

You have questions? We have
answers.

Last Reviewed: August 31, 2022

DEFENDANTS' EXHIBIT 78:

About CDC

Centers for Disease
Control and Prevention

About CDC Home

Mission, Role and Pledge

Vision

Equitably protecting health, safety & security.

CDC Moving Forward

In April 2022, CDC launched an effort to refine and modernize its structures, systems, and processes around developing and deploying our science and programs. The goal was to learn how to pivot our long-standing practices and adapt to pandemics and other public health emergencies, then to apply those lessons across the organization. The effort included a review of key workflows, with a particular focus on ensuring CDC's science reaches the public in an understandable, accessible, and implementable manner as quickly as possible.

Mission

CDC works 24/7 to protect America from health, safety and security threats, both foreign and in the U.S. Whether diseases start at home or abroad, are chronic or acute, curable or preventable, human error or deliberate attack, CDC fights disease and supports communities and citizens to do the same.

CDC increases the health security of our nation. As the nation's health protection agency, CDC saves lives and protects people from health threats. To accomplish our mission, CDC conducts critical science and provides health information that protects our nation against expensive and dangerous health threats, and responds when these arise.

Pledge to the American People

1. Be a diligent steward of the funds entrusted to our agency
2. Provide an environment for intellectual and personal growth and integrity
3. Base all public health decisions on the highest quality scientific data that is derived openly and objectively
4. Place the benefits to society above the benefits to our institution
5. Treat all persons with dignity, honesty, and respect

CDC in the 21st Century

- **On the cutting edge of health security** – confronting global disease threats through advanced computing and lab analysis of huge amounts of data to quickly find solutions.
- **Putting science into action** – tracking disease and finding out what is making people sick and the most effective ways to prevent it.
- **Helping medical care** – bringing new knowledge to individual health care and community health to save more lives and reduce waste.

CDC's Role



- Detecting and responding to new and emerging health threats
- Tackling the biggest health problems causing death and disability for Americans

- **Fighting diseases before they reach our borders** – detecting and confronting new germs and diseases around the globe to increase our national security.
- **Nurturing public health** – building on our significant contribution to have strong, well-resourced public health leaders and capabilities at national, state and local levels to protect Americans from health threats.
- Putting science and advanced technology into action to prevent disease
- Promoting healthy and safe behaviors, communities and environment
- Developing leaders and training the public health workforce, including disease detectives
- Taking the health pulse of our nation

DEFENDANTS' EXHIBIT 79:

About CDC

Centers for Disease
Control and Prevention[About CDC Home](#)

Office of Communications

Kevin Griffis

☐ Kevin Griffis is the Director of the Office of Communications (OC) at the Centers for Disease Control and Prevention (CDC). In this position, he leads and directs comprehensive communication outreach and delivery of CDC's health information and mission priorities along with managing risk communication and reputational issues for the agency. He serves as the principal public affairs leader and communication liaison for CDC, and coordinates agency-wide communication efforts by overseeing communication strategies and practices directed toward the public; news media; public health partners; governmental, national, and international organizations; and CDC staff.

Griffis served as Assistant Secretary for Public Affairs with the U.S. Department of Health and Human Services (HHS) under HHS Secretary Sylvia Burwell. There, he led a diversified public affairs team and spearheaded communication activities for a wide range of issues, including the department's response to the 2014 Ebola virus outbreak and the Zika virus outbreak. He was also instrumental in the implementation of the Affordable Care Act, and the rollout of the tobacco deeming rule.

Following his time at HHS, Griffis joined Planned Parenthood Federation of America in 2017 as vice president of Communications, where he led a large, interdisciplinary team at the forefront of reproductive health care delivery and advocacy for women's rights.

Most recently, Griffis worked for Centene Corporation, a multinational health care company that covers roughly one out of every 15 Americans and is ranked 26th on the Fortune 500 list. At Centene, he was vice president for Strategic Communications, working on messaging initiatives with the company's health plans in 30 states across the country.

Griffis first joined the Obama administration in March 2009 as director of public affairs for the U.S. Department of Commerce. There, he served through the BP/Deepwater Horizon oil spill and major policy initiatives, including the Recovery Act and the National Export Initiative. Prior to joining HHS, Griffis worked as communications director for U.S. Senator Cory Booker (D-NJ), and as communications director and senior advisor for Senator Booker's successful 2013 special election.

Griffis spent the first six years of his career covering government and politics as a reporter for newspapers in Maryland and Atlanta, GA. In Atlanta, he covered City Hall and the Georgia legislature for Creative Loafing newspaper from 2000-2004. Griffis holds a bachelor's degree from Beloit College in Wisconsin and grew up in the Snellville, GA area.

Last Reviewed: February 21, 2023

DEFENDANTS' EXHIBIT 80:

**IN THE UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF LOUISIANA**

**The State of Missouri and the State of
Louisiana,**

Plaintiffs,

v.

**President Joseph R. Biden, Jr., in his
official capacity as President of the United
States of America,**

et. al.,

Defendants.

Civil Action No. 22-cv-1213

DECLARATION OF CAROL CRAWFORD

I, Carol Crawford, declare the following, based on my personal knowledge, information acquired by me in the course of performing my official duties, and information contained in the records of the Centers for Disease Control and Prevention (“CDC”):

1. I have worked at CDC in various roles for 34 years. I currently serve as the Director for the Division of Digital Media within CDC’s Office of Communications, which until very recently was called the Office of the Associate Director for Communication (“OADC”). I have held that position since spring 2022. Before that, I was the Branch Chief of the Digital Media Branch within OADC (the work of that branch was transferred to the Division of Digital Media due to a reorganization of OADC that took place in spring 2022). I held that position from 2010 to spring 2022.

2. The CDC’s mission is to protect the health and safety of the American people. A core element of that mission is to promote awareness of science-based, data-driven information about

matters of public health. That includes addressing inaccurate information and beliefs on topics such as disease prevention and treatment. To that end, the CDC website maintains pages dedicated to addressing myths and facts about a wide range of topics. The examples are endless: the CDC website currently has fact sheets or “myths and facts” pages concerning, among other things, COVID-19 Vaccines¹; STDs and HIV²; community water fluoridation³; cholesterol⁴; smoking and tobacco use⁵; and *Bartonella* bacteria.⁶

3. The OADC supports the mission of CDC by ensuring the public health information provided by the agency is easily accessible and understandable to the public. That involves promoting CDC information through various online platforms, including the CDC’s own website and CDC social media pages. In my role, I provide leadership for CDC’s website and social media accounts, including convening personnel from across the agency to manage governance of the CDC website and social media pages, coordinating CDC’s web content management system, and drafting policies and guidelines in that space.

4. Before the onset of the COVID-19 pandemic in early 2020, I had occasional contacts with social media platforms as part of my role at OADC. The nature of those contacts was primarily to manage CDC’s own social media accounts. Generally speaking, outside the context of the COVID-19 pandemic, OADC’s work did not often involve direct interaction with social media companies; however, occasionally social media companies would reach out to OADC to partner with CDC on special projects (like promoting information about flu vaccines or

¹ <https://www.cdc.gov/coronavirus/2019-ncov/vaccines/facts.html>

² https://www.cdc.gov/tobacco/data_statistics/fact_sheets/fast_facts/index.htm

³ <https://www.cdc.gov/fluoridation/faqs/community-water-fluoridation.html>

⁴ https://www.cdc.gov/cholesterol/myths_facts.htm

⁵ https://www.cdc.gov/tobacco/data_statistics/fact_sheets/fast_facts/index.htm

⁶ <https://www.cdc.gov/bartonella/faq.html>

addressing prescription drug overdoses) or to highlight a new social media platform feature that CDC could use for its own social media accounts.

5. With the onset of the pandemic in early 2020, during the prior administration, I began having more frequent contact with social media platforms and technology companies such as Meta/Facebook and Google/YouTube. These discussions focused primarily on disseminating authoritative information concerning COVID-19 on their platforms. For example, social media platforms regularly reached out to CDC to ensure that the information the social media companies chose to promote on their platforms remained consistent with the latest CDC guidance on issues such as masking protocols or vaccine recommendations as CDC issued updates. Google, for instance, would reach out to ensure that its search results contained accurate links to the most up-to-date online guidance from CDC. Similarly, in another example, Facebook reached out to identify CDC content that could be linked on Facebook “groups” (i.e., a page on the platform for a community of users with a common interest, such as traveling or dogs).

6. During the pandemic, CDC began meeting regularly with certain social media companies to better facilitate these conversations in a pandemic environment where knowledge about and our understanding of the novel COVID-19 virus were evolving. Most of CDC’s meetings with these companies did not touch on misinformation. Any discussions about misinformation were focused on misinformation narratives that the companies or CDC observed circulating on platforms and the information available from CDC that would respond to those narratives. In these meetings, CDC did not ask a social media company to take any particular action with respect to any particular post. Currently, CDC does not meet or speak regularly with social media or technology companies to discuss misinformation, and has no current plans to do so, as discussed further below.

7. To be clear, there is still some occasional and indirect contact between CDC personnel and personnel from social media or technology companies that may touch on misinformation. CDC personnel develop periodic “State of Vaccine Confidence Insight” reports that are publicly posted (available at <https://www.cdc.gov/vaccines/covid-19/vaccinate-with-confidence.html>) and emailed to a wide list of recipients that may include personnel from social media companies. CDC funds, and CDC personnel attend and speak at, conferences that discuss misinformation and infodemic management; personnel from social media companies may also attend and/or speak at such conferences.⁷ I also note that CDC OADC has recently interacted with, and continues to interact with, social media companies to address accounts that impersonate CDC officials.

8. To the best of my knowledge, regular meetings between CDC personnel and Meta/Facebook personnel ended in the summer of 2021. While CDC communications personnel have had occasional and irregular meetings with Meta/Facebook personnel since then—for instance, a meeting in October 2022 about a potential in-kind contribution for COVID-19-related ads and recent meetings about functionalities for CDC to manage its own social media accounts—it has been well over a year since the last time a meeting touched on misinformation.

9. For a short period of time in 2021, CDC also met regularly with Pinterest to exchange information about COVID-19. To my knowledge, it has been well over a year since the last time CDC personnel had a meeting or communication with Pinterest personnel that touched on misinformation.

⁷ For example, CDC sponsored a workshop conducted by the National Academies of Sciences, Engineering, and Medicine entitled “Navigating Infodemics and Building Trust during Public Health Emergencies” (available at <https://www.nationalacademies.org/event/04-10-2023/navigating-infodemics-and-building-trust-during-public-health-emergencies-a-workshop#sectionEventMaterials>).

10. To the best of my knowledge, CDC has never had regular, recurring meetings with Twitter, but CDC did meet occasionally with Twitter in 2020 and 2021 to exchange information about COVID-19. Similarly, to my knowledge, it has been well over a year since the last time CDC personnel had a meeting or communication with Twitter personnel that touched on misinformation.

11. At times in the past and continuing to the present, CDC has also met regularly with Google. Generally speaking, the subject of those meetings was/is not misinformation; to the best of my knowledge, the last time a meeting with Google touched on misinformation was in March 2022. (My more recent meetings with Google have touched on topics such as the COVID-19 knowledge panel feature, and the impact of the redesign of the CDC.gov website on search engine results. And, for example, it is possible that other CDC components have met with Google sales teams to discuss ad buys.)

12. To the best of my knowledge, since March 2022, there has not been a meeting between CDC personnel and personnel from a social media or technology company where misinformation has been discussed at all, and there are no current plans to have such meetings in the future.

13. In the course of its efforts to address COVID-19 misinformation, CDC briefly engaged with the Census Bureau to receive assistance in monitoring the circulation of misinformation narratives on social and traditional media, so that CDC could better respond to those narratives with authoritative health information. (The Census Bureau developed experience with monitoring the circulation of misinformation in connection with the 2020 census.) The relevant Interagency Agreement ended over a year ago, and to the best of my knowledge, CDC's last meetings and communications with Census personnel about misinformation took place in summer 2021.

14. Pursuant to the Interagency Agreement, the Census Bureau assisted CDC with organizing and hosting two “Be On the Lookout” (“BOLO”) meetings with personnel from social media and technology companies in May 2021. CDC invited personnel from Meta/Facebook, Google/YouTube, and Twitter to attend the BOLO meetings. The purpose of the “BOLO” meetings was for CDC personnel to highlight prevalent COVID-19 misinformation narratives that CDC had identified and provide the companies with authoritative information on those topics. We presented PowerPoint slides discussing the narratives and the CDC-responsive information. The slides contained example social media posts illustrating the narratives. At these meetings, CDC did not ask social media companies to take any particular action with respect to specific posts. Rather, we provided information on COVID-19 misinformation narratives that the companies could use (or not use) as they saw fit.

15. In addition to the two May 2021 meetings, two more “BOLO” meetings were scheduled for summer of 2021 but never held. One was cancelled due to the Juneteenth holiday, and the second was cancelled because CDC had no information to share. No “BOLO” meeting has been held since May 28, 2021, and none are anticipated.

16. I also sent at least a couple of emails, unconnected to the above BOLO meetings, to social media companies with “BOLO” in the subject line. Similar to the information shared at the two May 2021 meetings, these emails notified platforms about a misinformation narrative about COVID-19 that CDC had observed circulating on the platforms. These were sent during mid- to late-2021; I have not sent any since 2021.⁸

⁸ I note that in August and November 2021, I and other CDC personnel met with/emailed individual platforms (Facebook and Twitter) to discuss misinformation around the Vaccine Adverse Events Reporting System (VAERS), a system that allows individuals to report to the CDC adverse health effects after receipt of a vaccine.

17. Throughout 2021, Facebook personnel sent CrowdTangle “content insights” reports to CDC. To my knowledge, that practice stopped in December 2021. These reports contained a summary of high-volume conversations on social media around COVID-19 topics. These reports helped give CDC insight into what information was circulating on social media regarding COVID-19; that would allow us to identify gaps in information and confusion about the facts concerning COVID-19, which were considerations we could take into account in developing CDC communications materials.

18. In one instance during the summer of 2021, a CDC employee used a Facebook reporting portal to identify four Facebook and Instagram posts containing vaccine misinformation. I am not aware of CDC personnel using that portal any other time. I am not aware of any efforts by CDC to inquire or investigate what happened to those posts, or of Facebook or Instagram informing CDC about what happened to those posts. CDC did not use this portal (beyond this one instance) because it did not seem like a worthwhile use of CDC time and resources nor were we comfortable reporting individual posts.

19. Personnel from Meta/Facebook and Google/YouTube occasionally sent emails to CDC soliciting CDC’s views on whether certain assertions about COVID-19 or other health topics were accurate or not. These assertions were not presented as particular posts, but rather as claims in the abstract. I (or someone from my team) responded to these emails on behalf of CDC after referring to publicly available information on CDC’s website or conferring with CDC subject-matter experts as appropriate. To the best of my current knowledge, the last such email CDC received from a social media company inquiring about the accuracy of certain assertions about health information was in summer 2022.

20. I am aware that plaintiffs in this action have asked for the following relief:

The Court should enter a preliminary injunction preventing Defendants, and their agents, officers, employees, contractors and all those acting in concert with them, from taking any steps to demand, urge, encourage, pressure, coerce, deceive, collude with, or otherwise induce any social-media company or platform for online speech, or any employee, officer, or agent of any such company or platform, to censor, suppress, remove, de-platform, suspend, shadow-ban, de-boost, deamplify, issue strikes against, restrict access to, demonetize, or take any similar adverse action against any speaker, content, or viewpoint expressed on social media. The Court should also preliminarily enjoin Defendants from acting in concert with any others, including but not limited to persons and entities associated with the Center for Internet Security, the Election Integrity Partnership, and the Virality Project, to engage in the aforementioned conduct, and from acting in concert with any such others who are engaged in any of the aforementioned conduct.

21. As noted above, a core part of CDC's mission is to promulgate science-based, data-driven information about public health matters. The broad injunction proposed by Plaintiffs could be construed to prohibit this core function. For instance, I am aware that some social media companies may choose to rely on CDC-promulgated information when determining what health-related content they will allow to circulate on their platforms, or to what extent they will allow it. Yet the proposed injunction is unclear as to whether it would prohibit CDC from publicly issuing a statement on a public health issue as a "step" to "encourage" a social media company to "suppress" or take "similar adverse action" against information that runs counter to the CDC-provided information. Thus, the injunction could inhibit CDC from performing its essential educational function, to the detriment of those whose health and well-being (and perhaps their lives) depend on the availability of accurate information about disease prevention and treatment.

22. CDC also funds research and other public health programs through billions of dollars' worth of grants and cooperative agreements. That entire enterprise could be thrown into jeopardy by an injunction of the type proposed by plaintiffs. For example, if a CDC-funded entity publicizes research that runs contrary to a narrative circulating on social media, and a social media company then takes steps consistent with its terms of service to limit that narrative, then it

is unclear whether CDC would be deemed, in the injunction's words, to be "acting in concert" with "others" "engaged" in the "conduct" of "inducing" a social-media company to "suppress" or take "similar adverse action" against certain content, speakers, or viewpoints. In this respect, as well, the injunction if issued could inhibit CDC from carrying out core elements of its mission that are important to public health.

23. Put simply, it appears that many public-facing actions by the CDC—that is, actions that are not purely internal to the agency—that involve the promotion of science-based, data-driven public health information could be construed to violate the injunction proposed by plaintiffs. Thus, it will be very difficult for CDC to determine what conduct does or does not fall within the scope of such an injunction—particularly where it has no control over actions taken by third parties, such as social media companies and others who may rely upon CDC's publications and statements concerning public health matters. Moreover, if CDC is unable to carry out its mission of promulgating science-based, data-driven information about public health matters, and making that information publicly understandable and accessible, then all of society would suffer, because the public would be deprived of critical information needed to protect it from a host of diseases and other public health threats.

Pursuant to 28 U.S.C. § 1746, I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct to the best of my knowledge.

Executed on this _____ day of April, 2023, in Atlanta, Georgia,

Carol

Crawford -S

Digitally signed by Carol
Crawford -S
Date: 2023.04.26 08:29:05
-04'00'

CAROL CRAWFORD

Health Communications Specialist

Director, Division of Digital Media

Office of the Associate Director for Communication

Centers for Disease Control and Prevention

DEFENDANTS' EXHIBIT 81:



Home Policy Analysis Rapid Response Weekly Briefings

Our weekly briefings summarize key narratives of online anti-vaccine misinformation. Please note that these briefings are not exhaustive. Instead, we aim to highlight critical trends in anti-vaccine discussion each week based on engagement, novelty, spread, and requests from stakeholder partners.

We intend for these briefings to provide situational awareness of key anti-vaccine narratives and to help guide public health messaging that is responsive to online conversations. These briefings do occasionally contain direct links to misinformation. Following [guidelines by Data & Society](#), we recommend that you do not publicize or spread those links, even when criticizing them. For additional information on how to responsibly report on misinformation, check out [these helpful resources from First Draft](#).

[Virality Project Weekly Briefing 32 – August 3, 2021](#)

[Virality Project Weekly Briefing 31 – July 27, 2021](#)

[Virality Project Weekly Briefing 30 – July 20, 2021](#)

[Virality Project Weekly Briefing 29 – July 13, 2021](#)

[Virality Project Weekly Briefing 28 – July 7, 2021](#)

[Virality Project Weekly Briefing 27 – June 29, 2021](#)

[Virality Project Weekly Briefing 26 – June 22, 2021](#)

[Virality Project Weekly Briefing 25 – June 15, 2021](#)

[Virality Project Weekly Briefing 24 – June 8, 2021](#)

[Virality Project Weekly Briefing 23 – June 2, 2021](#)

[Virality Project Weekly Briefing 22 – May 25, 2021](#)

[Virality Project Weekly Briefing 21 – May 18, 2021](#)

[Virality Project Weekly Briefing 20 – May 11, 2021](#)

[Virality Project Weekly Briefing 19 – May 4, 2021](#)

[Virality Project Weekly Briefing 18 – April 27, 2021](#)

[Virality Project Weekly Briefing 17 – April 20, 2021](#)

[Virality Project Weekly Briefing 16 – April 13, 2021](#)

[Virality Project Weekly Briefing 15 – April 6, 2021](#)

[Virality Project Weekly Briefing 14 – March 30, 2021](#)

[Virality Project Weekly Briefing 13 – March 23, 2021](#)

[Virality Project Weekly Briefing 12 – March 16, 2021](#)

[Virality Project Weekly Briefing 11 – March 9, 2021](#)

[Virality Project Weekly Briefing 10 – March 2, 2021](#)

[Virality Project Weekly Briefing 9 – February 23, 2021](#)

[Virality Project Weekly Briefing 8 – February 16, 2021](#)

[Virality Project Weekly Briefing 7 – February 9, 2021](#)

[Virality Project Weekly Briefing 6 – February 2, 2021](#)

[Virality Project Weekly Briefing 5 – January 26, 2021](#)

[Virality Project Weekly Briefing 4 – January 19, 2021](#)

DEFENDANTS' EXHIBIT 82:



Home Policy Analysis Rapid Response Weekly Briefings



How Debunked Science Spreads

[Read More](#)



7/29/21

Content moderation avoidance strategies

[Read More](#)



7/23/21

Around and Back Again: How Anti-Vaccine Narratives Go Global

[Read More](#)



7/20/21

How Russia and China attempt to influence US vaccine conversations

[Read More](#)



6/25/21

Fauxi: Undermining Authoritative Health Sources

[Read More](#)



6/24/21

Made to Stick: Origins and Spread of the Magnetic Vaccine Narrative

[Read More](#)



5/11/21

Rapid Response: Expanding COVID-19 Vaccines to Children

[Read More](#)



4/27/21

Vaccine “shedding” narratives targeted toward women

[Read More](#)



4/17/21

J&J Suspension Rapid Response

[Read More](#)



4/7/21

Mark of the Beast meets Vaccine Passports

The claim that vaccine passports are potentially the mark of the beast has received viral coverage in the past week primarily due to Congresswoman Greene's statement. This claim aligns with her history of promoting conspiratorial claims and ideas, including QAnon. his claim has larger implications for vaccine hesitancy beyond the association between vaccine passports and "the mark."

[Read More](#)



3/29/21

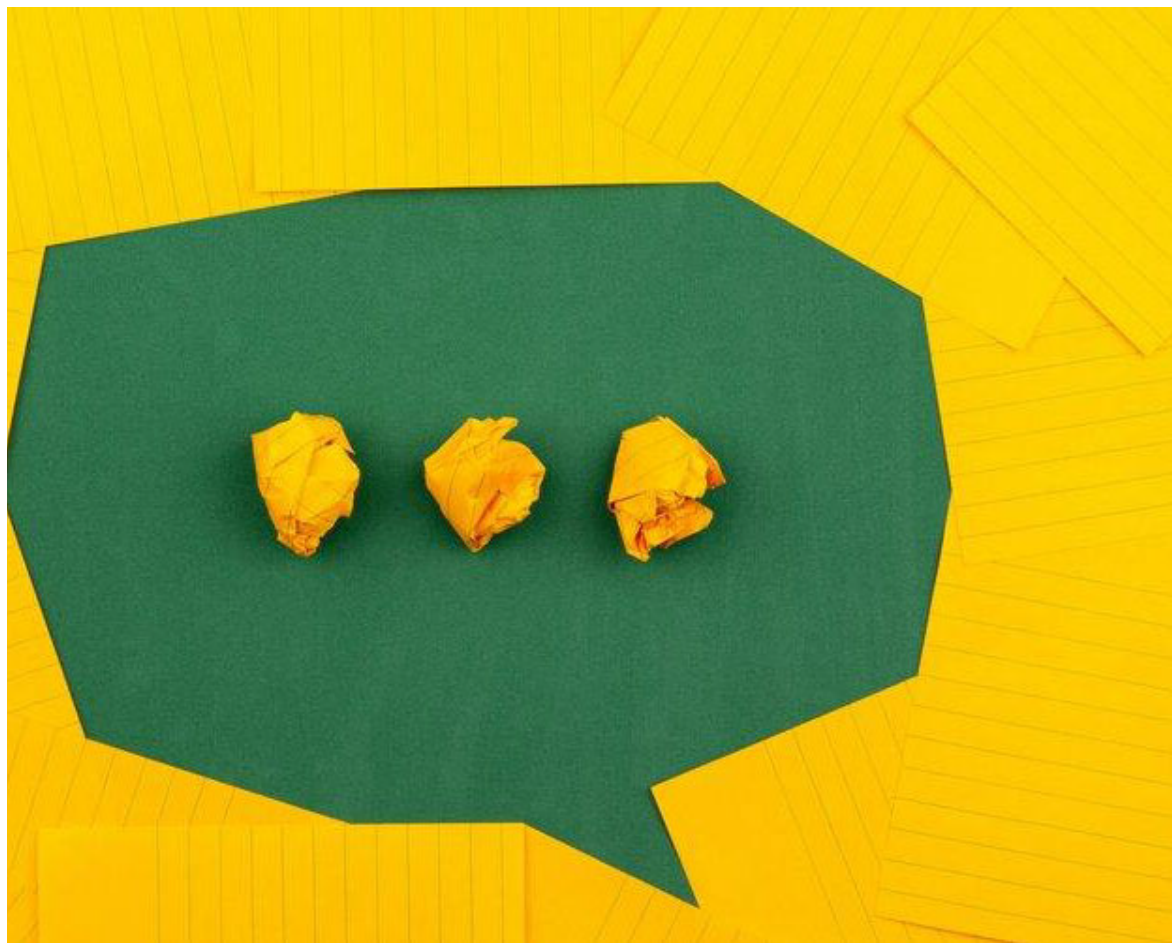
The Vaccine Passport Narrative in Vaccine Hesitant Communities

[Read More](#)

DEFENDANTS' EXHIBIT 83:



Home Policy Analysis Rapid Response Weekly Briefings



New Truths, Old Lies ?

[Read More](#)

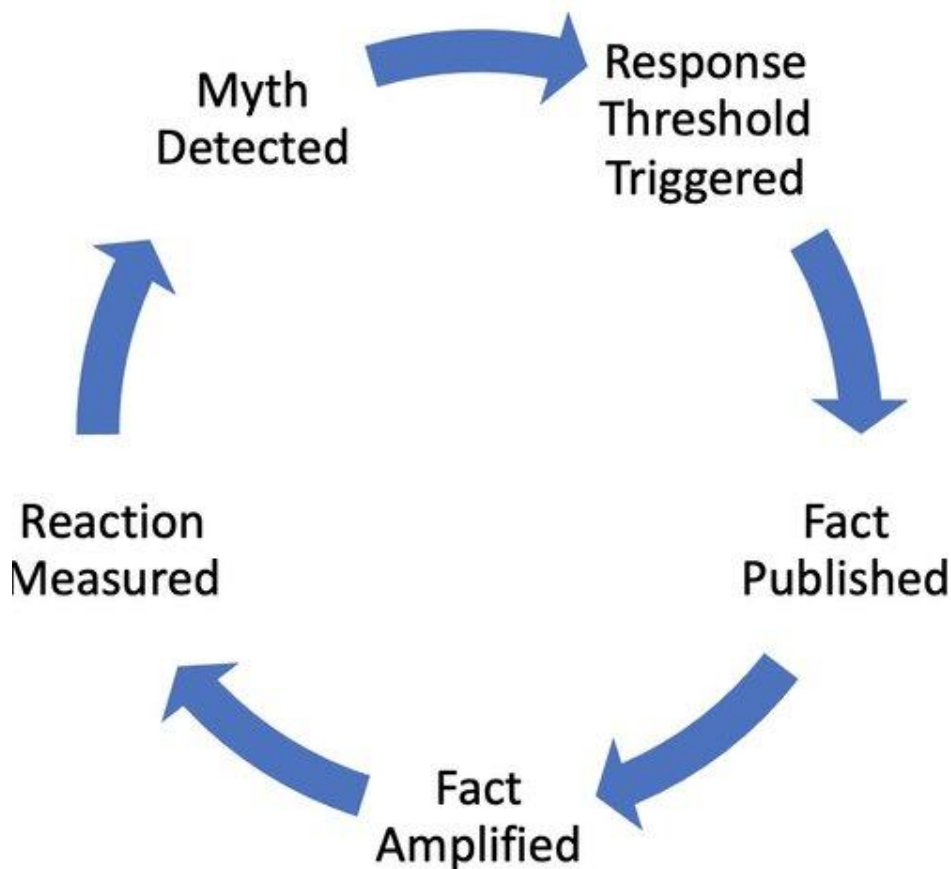


7/8/21

The Case for a Mis- and Disinformation Center of Excellence

How the federal government can better coordinate to address the threat of mis- and disinformation.

[Read More](#)

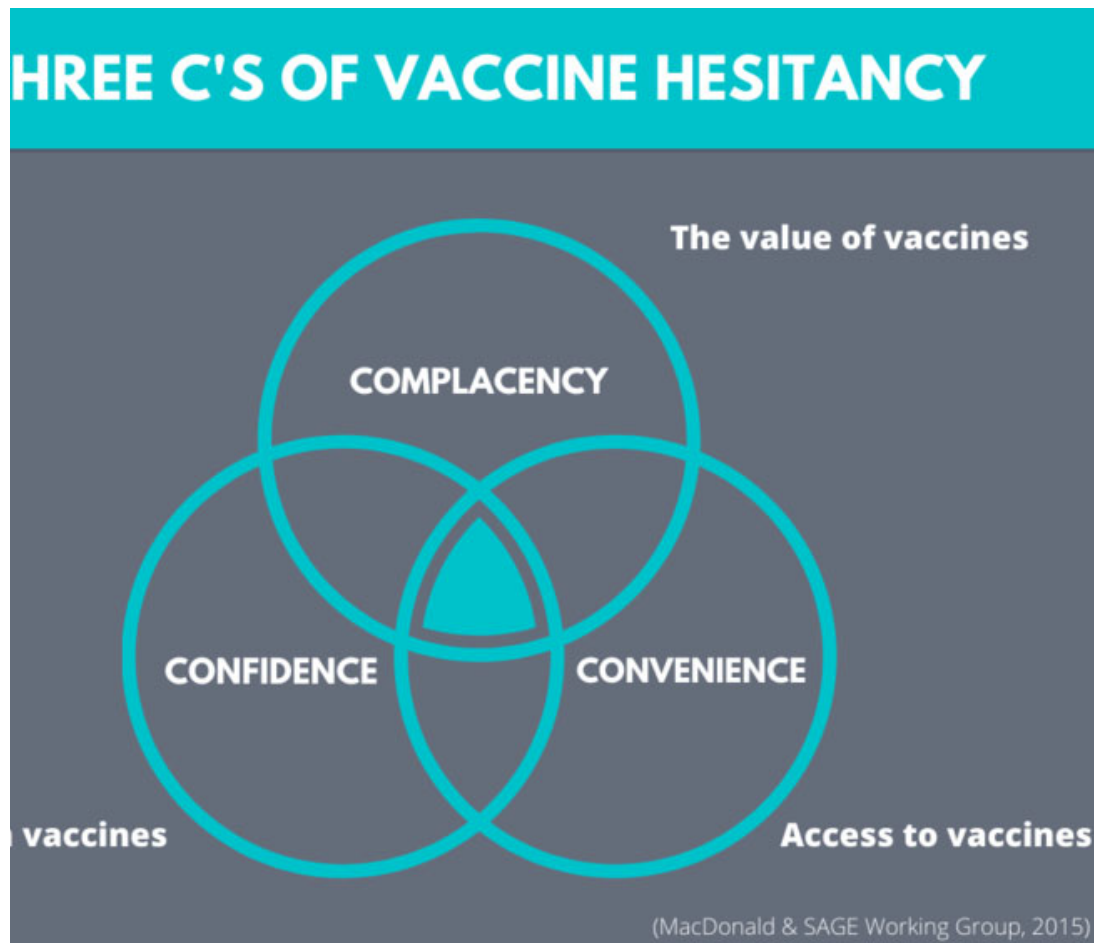


5/4/21

Rumor Control: a Framework for Countering Vaccine Misinformation

As adult vaccination rates plateau, vaccine misinformation is likely to surge. Rumor Control pages could offer public health communicators a tool to fight back.

[Read More](#)



3/4/21

Vaccine Rollout and Mis/Disinformation: Expectations and Action Plan for Health Communicators

[Read More](#)

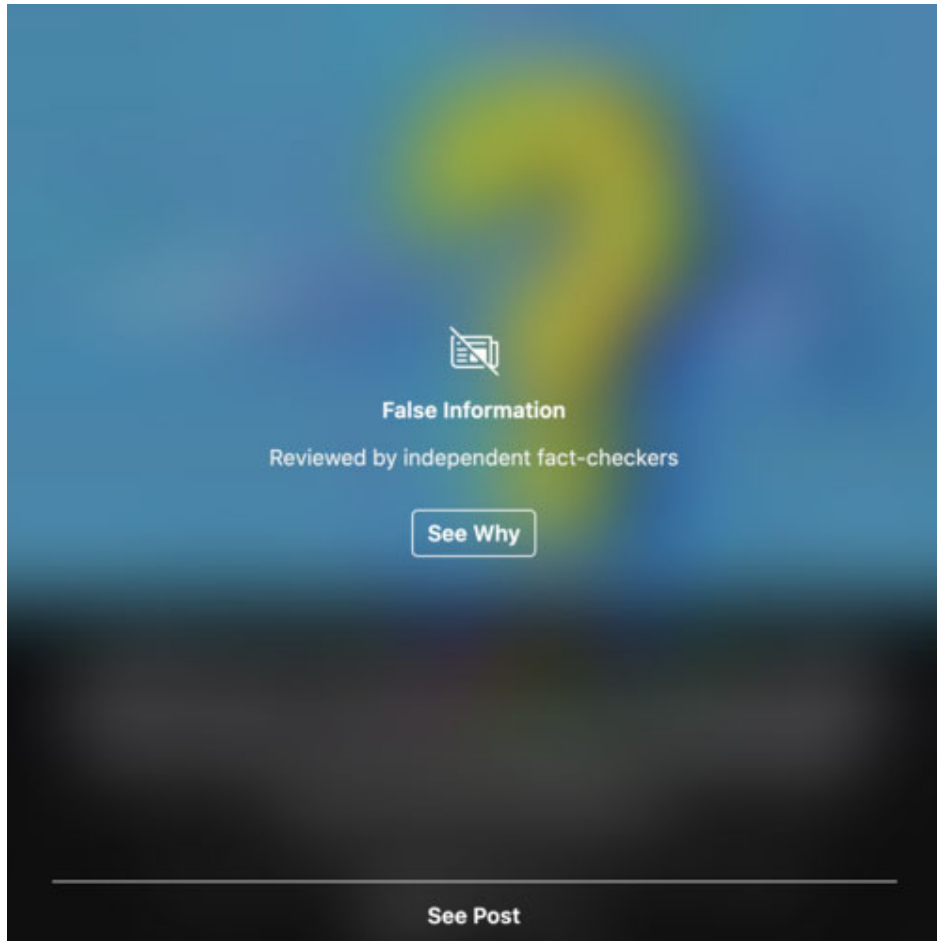


2/18/21

White House COVID-19 Vaccine Communication Plan: Analysis and Recommendations

The White House has a plan to counter vaccine misinformation. We recommend some targeted actions to bolster it.

[Read More](#)



2/11/21

Evaluating COVID-19 Vaccine Policies on Social Media Platforms

[Read More](#)

DEFENDANTS' EXHIBIT 84:

NewsRoom

4/5/18 USA TODAY 03B
2018 WLNR 10231713

USA Today (USA)
Copyright (c) 2018 USA Today

April 5, 2018

Section: MONEY

Many YouTube creators frustrated by changes in policies, practices

Brett Molina, USA TODAY

A shooting at YouTube's headquarters in California has sparked questions about recent changes the video service made to how its creators get paid.

Authorities have identified the suspect as Nasim Aghdam, 39, accused of shooting three people before apparently taking her own life.

Police say Aghdam's apparent motive for the shooting was frustration with the policies and practices of YouTube. Social media posts made by Aghdam, along with comments made by her father, suggest the shooter was "angry" because YouTube had stopped paying her for videos.

Although YouTube does not directly pay its content creators, users can make money through ads that run on their video or subscriptions collected by YouTube Red premium service. However, recent policy changes have rankled many creators.

Here's a breakdown of how YouTube creators can make money:

What is monetization? For YouTube, it's a way for creators to make money off their videos. YouTube hosts a Partners Program, where creators earn money from ads appearing on their videos or Red subscriptions. The ads run through AdSense, Google's platform for serving ads to websites including YouTube.

For its bigger names, making a living through YouTube can prove lucrative. According to Forbes, the highest-paid YouTube star, Daniel Middleton, raked in \$16.5 million in income last year thanks to his channel DanTDM.

What are the changes users seem upset about? Last April, YouTube updated its Partners Program to no longer serve ads on videos until a channel reaches 10,000 lifetime views. It also revealed work on a review process for new members of the program.

The change was made in response to tactics such as channels taking original videos and uploading them again to rake in ad money.

"We want creators of all sizes to find opportunity on YouTube, and we believe this new application process will help ensure creator revenue continues to grow and end up in the right hands," Ariel Bardin, YouTube's vice president of product management, said in a blog post last April.

In January, YouTube boosted those thresholds to 4,000 hours of watch time over the last 12 months and 1,000 subscribers. As of Feb. 20, any channels below these requirements could no longer make money through ads.

Why did YouTube make these changes? Major advertisers including AT&T and Verizon started pulling their business from YouTube in March 2017 after discovering their ads were appearing on offensive or extremist videos. YouTube parent company Google said it would start an "extensive review" of its ad policies. Last August, YouTube said it was working more quickly to pull terrorist content from its site.

What did this mean for YouTube creators? If you were an established YouTube star with millions of followers, the policy didn't change things. But smaller channels on the edges of YouTube's thresholds were shut out.

Although YouTube acknowledged in January a significant number of channels would be affected by the change, it said 99% of affected channels were making less than \$100 a year in the last year.

Those changes arrived as it weathered controversy surrounding one of its biggest names, Logan Paul. In February, the vlogger saw ads on his channel suspended temporarily after uploading a video of him shocking a rat with a taser.

---- Index References ----

Industry: (Digital Broadcasting (1DI81); Entertainment (1EN08); Internet (1IN27); Internet Audio & Video (1IN30); Internet Media (1IN67); Internet Technology (1IN39); Online Social Media (1ON38); TV (1TV19); TV Programming (1TV26))

Language: EN

Edition: FINAL

Word Count: 527

End of Document

© 2023 Thomson Reuters. No claim to original U.S. Government Works.

NewsRoom

DEFENDANTS' EXHIBIT 85:

INSTITUTES AT NIH

List of Institutes and Centers

NIH Institutes

National Cancer Institute (NCI) — Est. 1937

NCI leads a national effort to eliminate the suffering and death due to cancer. Through basic and clinical biomedical research and training, NCI conducts and supports research that will lead to a future in which we can prevent cancer before it starts, identify cancers that do develop at the earliest stage, eliminate cancers through innovative treatment interventions, and biologically control those cancers that we cannot eliminate so they become manageable, chronic diseases.

National Eye Institute (NEI) — Est. 1968

The National Eye Institute's mission is to conduct and support research, training, health information dissemination, and other programs with respect to blinding eye diseases, visual disorders, mechanisms of visual function, preservation of sight, and the special health problems and requirements of the blind.

National Heart, Lung, and Blood Institute (NHLBI) — Est. 1948

The National Heart, Lung, and Blood Institute (NHLBI) provides global leadership for a research, training, and education program to promote the prevention and treatment of heart, lung, and blood diseases and enhance the health of all individuals so that they can live longer and more fulfilling lives. The NHLBI stimulates basic discoveries about the causes of disease, enables the translation of basic discoveries into clinical practice, fosters training and mentoring of emerging scientists and physicians, and communicates research advances to the public.

National Human Genome Research Institute (NHGRI) — Est. 1989

NHGRI is devoted to advancing health through genome research. The Institute led NIH's contribution to the Human Genome Project, which was successfully completed in 2003 ahead of schedule and under budget. Building on the foundation laid by the sequencing of the human genome, NHGRI's work now encompasses a broad range of research aimed at expanding understanding of human biology and improving human health. In addition, a critical part of NHGRI's mission continues to be the study of the ethical, legal and social implications of genome research.

National Institute on Aging (NIA) — Est. 1974

NIA leads a national program of research on the biomedical, social, and behavioral aspects of the aging process; the prevention of age-related diseases and disabilities; and the promotion of a better quality of life for all older Americans.

National Institute on Alcohol Abuse and Alcoholism (NIAAA) — Est. 1970

NIAAA conducts research focused on improving the treatment and prevention of alcoholism and alcohol-related problems to reduce the enormous health, social, and economic consequences of this disease.

National Institute of Allergy and Infectious Diseases (NIAID) — Est. 1948

NIAID research strives to understand, treat, and ultimately prevent the myriad infectious, immunologic, and allergic diseases that threaten millions of human lives.

National Institute of Arthritis and Musculoskeletal and Skin Diseases (NIAMS) — Est. 1986

NIAMS supports research into the causes, treatment, and prevention of arthritis and musculoskeletal and skin diseases, the training of basic

and clinical scientists to carry out this research, and the dissemination of information on research progress in these diseases.

National Institute of Biomedical Imaging and Bioengineering (NIBIB) — Est. 2000

The mission of the National Institute of Biomedical Imaging and Bioengineering (NIBIB) is to transform through engineering the understanding of disease and its prevention, detection, diagnosis, and treatment.

Eunice Kennedy Shriver National Institute of Child Health and Human Development (NICHD) — Est. 1962

NICHD leads research and training to understand human development, improve reproductive health, enhance the lives of children and adolescents, and optimize abilities for all.

National Institute on Deafness and Other Communication Disorders (NIDCD) — Est. 1988

NIDCD conducts and supports biomedical research and research training on normal mechanisms as well as diseases and disorders of hearing, balance, smell, taste, voice, speech, and language that affect 46 million Americans.

National Institute of Dental and Craniofacial Research (NIDCR) — Est. 1948

NIDCR provides leadership for a national research program designed to understand, treat, and ultimately prevent the infectious and inherited craniofacial-oral-dental diseases and disorders that compromise millions of human lives.

National Institute of Diabetes and Digestive and Kidney Diseases (NIDDK) — Est. 1950

The mission of the National Institute of Diabetes and Digestive and Kidney Diseases (NIDDK) is to conduct and support medical research and research training and to disseminate science-based information on diabetes and other endocrine and metabolic diseases; digestive diseases, nutritional disorders, and obesity; and kidney, urologic, and hematologic diseases, to improve people's health and quality of life.

National Institute on Drug Abuse (NIDA) — Est. 1974

The mission of the National Institute on Drug Abuse (NIDA) is to advance science on the causes and consequences of drug use and addiction and to apply that knowledge to improve individual and public health.

National Institute of Environmental Health Sciences (NIEHS) — Est. 1969

The mission of the National Institute of Environmental Health Sciences is to discover how the environment affects people in order to promote healthier lives.

National Institute of General Medical Sciences (NIGMS) — Est. 1962

The National Institute of General Medical Sciences (NIGMS) supports basic research that increases understanding of biological processes and lays the foundation for advances in disease diagnosis, treatment and prevention. NIGMS-funded scientists investigate how living systems work at a range of levels, from molecules and cells to tissues, whole organisms and populations. The Institute also supports research in certain clinical areas, primarily those that affect multiple organ systems. To assure the vitality and continued productivity of the research enterprise, NIGMS provides leadership in training the next generation of scientists, in enhancing the diversity of the scientific workforce, and in developing research capacities throughout the country.

National Institute of Mental Health (NIMH) — Est. 1949

NIMH provides national leadership dedicated to understanding, treating, and preventing mental illnesses through basic research on the brain and behavior, and through clinical, epidemiological, and services research.

National Institute on Minority Health and Health Disparities (NIMHD) — Est. 2010

NIMHD has a long history, beginning in 1990 as an Office and later designated a Center in 2000. The mission of NIMHD is to lead scientific research to improve minority health and eliminate health disparities. To accomplish its mission, NIMHD plans, reviews, coordinates, and evaluates all minority health and health disparities research and activities of the National Institutes of Health; conducts and supports research in minority health and health disparities; promotes and supports the training of a diverse research workforce; translates and disseminates research information; and fosters innovative collaborations and partnerships.

National Institute of Neurological Disorders and Stroke (NINDS) — Est. 1950

The mission of NINDS is to seek fundamental knowledge about the brain and nervous system and to use that knowledge to reduce the burden of neurological disease. To accomplish this goal the NINDS supports and conducts basic, translational, and clinical research on the normal and diseased nervous system. The Institute also fosters the training of investigators in the basic and clinical neurosciences, and seeks better understanding, diagnosis, treatment, and prevention of neurological disorders.

National Institute of Nursing Research (NINR) — Est. 1986

The mission of the National Institute of Nursing Research (NINR) is to lead nursing research to solve pressing health challenges and inform practice and policy—optimizing health and advancing health equity into the future.

National Library of Medicine (NLM) — Est. 1956

NLM collects, organizes, and makes available biomedical science information to scientists, health professionals, and the public. The Library's Web-based databases, including PubMed/Medline and MedlinePlus, are used extensively around the world. NLM conducts and supports research in biomedical communications; creates information resources for molecular biology, biotechnology, toxicology, and environmental health; and provides grant and contract support for training, medical library resources, and biomedical informatics and communications research.

NIH Centers

NIH Clinical Center (CC) — Est. 1953

The NIH Clinical Center, America's research hospital, provides a versatile clinical research environment enabling the NIH mission to improve human health by investigating the pathogenesis of disease; conducting first-in-human clinical trials with an emphasis on rare diseases and diseases of high public health impact; developing state-of-the-art diagnostic, preventive, and therapeutic interventions; training the current and next generations of clinical researchers; and, ensuring that clinical research is ethical, efficient, and of high scientific quality.

Center for Information Technology (CIT) — Est. 1964

CIT incorporates the power of modern computers into the biomedical programs and administrative procedures of the NIH by focusing on three primary activities: conducting computational biosciences research, developing computer systems, and providing computer facilities.

Center for Scientific Review (CSR) — Est. 1946

CSR is the portal for NIH grant applications and their review for scientific merit. CSR oversees and implements peer review for over 75% of the more than 88,000 applications submitted to NIH each year, as well as for some other components of HHS. The mission of CSR is to see that NIH grant applications receive fair, independent, expert, and timely scientific reviews — free from inappropriate influences — so NIH can fund the most promising research.

Fogarty International Center (FIC) — Est. 1968

FIC promotes and supports scientific research and training internationally to reduce disparities in global health.

National Center for Advancing Translational Sciences (NCATS) — Est. 2011

The mission of NCATS is to catalyze the generation of innovative methods and technologies that will enhance the development, testing, and implementation of diagnostics and therapeutics across a wide range of human diseases and conditions.

National Center for Complementary and Integrative Health (NCCIH) — Est. 1999

The mission of NCCIH is to define, through rigorous scientific investigation, the usefulness and safety of complementary and integrative health interventions and their roles in improving health and health care.

This page last reviewed on June 16, 2022

Quick Links



NIH...Turning Discovery Into Health®

National Institutes of Health, 9000 Rockville Pike, Bethesda, Maryland 20892

U.S. Department of Health and Human Services

DEFENDANTS' EXHIBIT 87:



NIAID Mission

NIAID conducts and supports basic and applied research to better understand, treat, and ultimately prevent infectious, immunologic, and allergic diseases. For more than 60 years, NIAID research has led to new therapies, vaccines, diagnostic tests, and other technologies that have improved the health of millions of people in the United States and around the world.

In fiscal year 2021, the NIAID budget was \$6.1 billion. The Institute dedicated these funds to support scientific opportunities that align with its mission and address domestic and global health problems and diseases.

Among the 27 Institutes and Centers that comprise the National Institutes of Health, NIAID has a unique mandate, which requires the Institute to respond to emerging public health threats. Toward this end, NIAID manages a complex and diverse research portfolio that aims to do the following:

- Expand the breadth and depth of knowledge in all areas of infectious, immunologic, and allergic diseases
- Develop flexible domestic and international research capacities to respond appropriately to emerging and re-emerging disease threats at home and abroad

NIAID advances the understanding, diagnosis, and treatment of many of the world's most intractable and widespread diseases. Key research areas include newly emerging and re-emerging infectious diseases such as tuberculosis and influenza, HIV/AIDS, biodefense, and immune-mediated diseases including asthma and allergy.

Content last reviewed on April 16, 2021

DEFENDANTS' EXHIBIT 88:



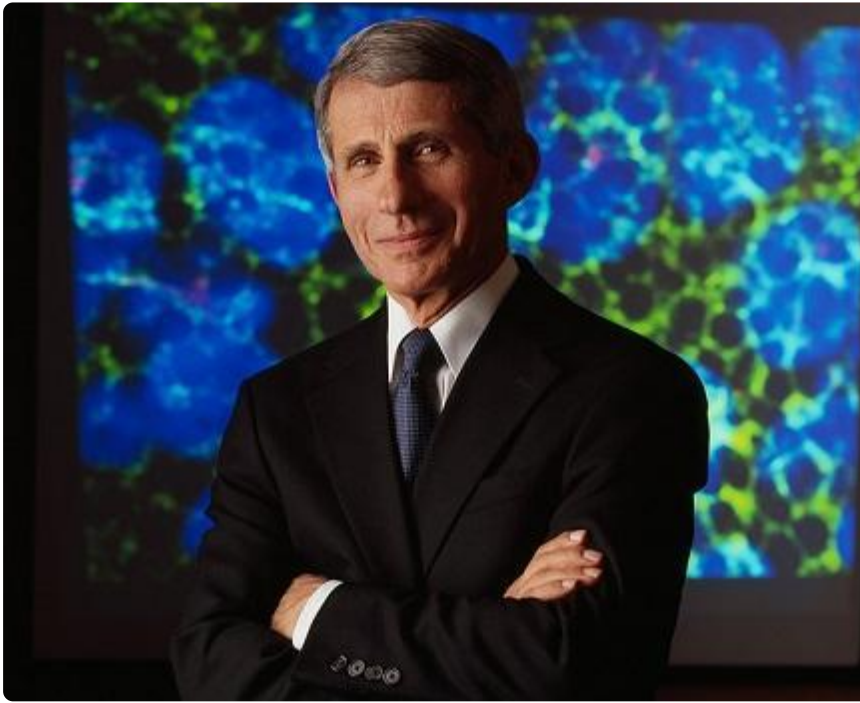
Anthony S. Fauci, M.D., Former NIAID Director

Dr. Fauci served as NIAID Director from 1984 to 2022. He oversaw an extensive research portfolio of basic and applied research to prevent, diagnose, and treat established infectious diseases such as HIV/AIDS, respiratory infections, diarrheal diseases, tuberculosis, and malaria as well as emerging diseases such as Ebola, Zika, and COVID-19. He also led the NIAID research effort on transplantation and immune-related illnesses, including autoimmune disorders, asthma, and allergies.

Dr. Fauci advised seven Presidents on HIV/AIDS and many other domestic and global health issues. He was one of the principal architects of the President's Emergency Plan for AIDS Relief (PEPFAR), a program that has saved more than 20 million lives throughout the developing world.

[Read Dr. Fauci's Biography \(/node/9753\)](#)

[Read about how NIAID is conducting and supporting research on SARS CoV-2 and the disease COVID-19 \(/diseases-conditions/coronaviruses\)](#)



NIAID Director Anthony S. Fauci, M.D.

Credit: NIAID

Profiles, Awards, and Honors

December 1, 2022

Journal of Infectious Diseases — Thank You — Tony Fauci [↗](https://bit.ly/3gGj7jZ) (https://bit.ly/3gGj7jZ)

June 11, 2022

Holy Cross Names Science Complex for Anthony Fauci '62, Hon. '87 [↗](https://bit.ly/3mJ254h)
(https://bit.ly/3mJ254h)

February 15, 2021

Dr. Fauci awarded the Dan David Prize for Public Health [↗](https://www.dandavidprize.org/)
(https://www.dandavidprize.org/)

See all Profiles, Awards and Honors [➤ \(/director/awards\)](/director/awards)

Publications and Articles

December 10, 2022

Anthony Fauci — A Message to the Next Generation of Scientists [↗](#)

(<https://www.nytimes.com/2022/12/10/opinion/anthony-fauci-retirement.html?searchResultPosition=1>)

November 30, 2022

Forty Years of Investment in HIV Research — Progress Towards Ending the HIV Pandemic and Preparation for Future Pandemics [↗](#)

(<https://pubmed.ncbi.nlm.nih.gov/36448551/>)

November 26, 2022

It Ain't Over Till It's Over...but It's Never Over — Emerging and Reemerging Infectious Diseases [↗](#) (<https://www.nejm.org/doi/full/10.1056/NEJMp2213814>)

See all Publications and Articles [➤ \(/director/publications\)](#)

Dr. Fauci in the News

October 22, 2022

Good Morning America — Dr. Fauci discusses surge in RSV cases [↗](#)

(<https://abcn.ws/3z3AWzx>)

October 21, 2022

Infectious Disease News — IDSA announces courage award honoring Dr. Fauci [↗](#)

(<https://bit.ly/3zexvpG>)

WNYC/The Brian Lehrer Show — The Status (and Reflections) of the Pandemic with Dr. Fauci [↗](#) (<https://bit.ly/3VSWTet>)

See all Dr. Fauci in the News [➤ \(/news-events/director-in-the-news\)](/news-events/director-in-the-news)

Congressional Testimony

September 14, 2022 [↗](#)

(<https://www.help.senate.gov/download/testimony/fauci-testimony91622>)

Videocast and Testimony: The Role of the National Institute of Allergy and Infectious Diseases in Research Addressing the Monkeypox Public Health Emergency. Senate Committee on Health, Education, Labor, and Pensions hearing, “Stopping the Spread of Monkeypox: Examining the Federal Response.

Videocast of Congressional Testimony from September 14, 2022 [↗](#)

(<https://www.help.senate.gov/hearings/stopping-the-spread-of-monkeypox-examining-the-federal-response>)

June 16, 2022 [↗](#)

(<https://www.help.senate.gov/download/testimony/fauci-testimony61622>)

Videocast and Testimony: The Role of the National Institute of Allergy and Infectious Diseases in Research to Address the COVID-19 Pandemic. Senate Committee on Health, Education, Labor, and Pensions hearing: “An Update on the Ongoing Federal Response to COVID-19: Current Status and Future Planning.”

Videocast of Congressional Testimony from June 16, 2022 [↗](#)

(<https://www.help.senate.gov/hearings/an-update-on-the-ongoing-federal-response-to-covid-19-current-status-and-future-planning>)

See all Congressional Testimonies [➤ \(/news-events/congressional-testimony\)](/news-events/congressional-testimony)

Laboratory of Immunoregulation

Dr. Fauci also is the long-time chief of the Laboratory of Immunoregulation (LIR). He has made many contributions to basic and clinical research on the pathogenesis and treatment of immune-mediated and infectious diseases. He helped pioneer the field of human immunoregulation by making important basic scientific observations that underpin the current understanding of the regulation of the human immune response.

Read more about LIR (</research/lab-immunoregulation>)

DEFENDANTS' EXHIBIT 89:



Statement by Anthony S. Fauci, M.D.

August 22, 2022

I am announcing today that I will be stepping down from the positions of Director of the National Institute of Allergy and Infectious Diseases (NIAID) and Chief of the NIAID Laboratory of Immunoregulation, as well as the position of Chief Medical Advisor to President Joe Biden. I will be leaving these positions in December of this year to pursue the next chapter of my career.

It has been the honor of a lifetime to have led the NIAID, an extraordinary institution, for so many years and through so many scientific and public health challenges. I am very proud of our many accomplishments. I have worked with – and learned from – countless talented and dedicated people in my own laboratory, at NIAID, at NIH and beyond. To them I express my abiding respect and gratitude.

Over the past 38 years as NIAID Director, I have had the enormous privilege of serving under and advising seven Presidents of the United States, beginning with President Ronald Reagan, on newly emerging and re-emerging infectious disease threats including HIV/AIDS, West Nile virus, the anthrax attacks, pandemic influenza, various bird influenza threats, Ebola and Zika, among others, and, of course, most recently the COVID-19 pandemic. I am particularly proud to have served as the Chief Medical Advisor to President Joe Biden since the very first day of his administration.

While I am moving on from my current positions, I am not retiring. After more than 50 years of government service, I plan to pursue the next phase of my career while I still have so much energy and passion for my field. I want to use what I have learned as NIAID Director

to continue to advance science and public health and to inspire and mentor the next generation of scientific leaders as they help prepare the world to face future infectious disease threats.

Over the coming months, I will continue to put my full effort, passion and commitment into my current responsibilities, as well as help prepare the Institute for a leadership transition. NIH is served by some of the most talented scientists in the world, and I have no doubt that I am leaving this work in very capable hands.

Thanks to the power of science and investments in research and innovation, the world has been able to fight deadly diseases and help save lives around the globe. I am proud to have been part of this important work and look forward to helping to continue to do so in the future.

Contact

Submit a Media Request

Contact the NIAID News & Science Writing Branch.

301-402-1663 📞

niaidnews@niaid.nih.gov ✉

All Media Contacts (/news-events/media-contacts)

Related Content

[Anthony S. Fauci, M.D. \(/research/anthony-s-fauci-md\)](/research/anthony-s-fauci-md)

[Anthony S. Fauci, M.D. \(/about/anthony-s-fauci-md-bio\)](/about/anthony-s-fauci-md-bio)

[NIAID Council Minutes — January 25, 2021 \(/about/niaid-council-minutes-january-25-2021\)](/about/niaid-council-minutes-january-25-2021)

[Dr. Fauci Reflects on the Perpetual Challenge of Infectious Diseases \(/news-events/dr-fauci-reflects-perpetual-challenge-infectious-diseases\)](/news-events/dr-fauci-reflects-perpetual-challenge-infectious-diseases)

[NIAID Council Minutes — September 17, 2018 \(/about/niaid-council-minutes-september-17-2018\)](/about/niaid-council-minutes-september-17-2018)

Content last reviewed on August 22, 2022

DEFENDANTS' EXHIBIT 90:

This is historical material, "frozen in time." The web site is no longer updated and links to external web sites and some internal pages will not work.



THE WHITE HOUSE
PRESIDENT GEORGE W. BUSH

[Home](#) > [News & Policies](#) > [June 2008](#)

For Immediate Release
Office of the Press Secretary
June 19, 2008

President Bush Honors Presidential Medal of Freedom Recipients

East Room

[In Focus: Freedom Agenda](#)

[2008 Presidential Medal of Freedom Citations](#)

9:45 A.M. EDT

THE PRESIDENT: Welcome to the White House, for what is going to be a joyous occasion. Mr. Vice President, Justice Scalia, members of my Cabinet and administration, members of Congress, Medal of Freedom recipients and their families and friends: Thanks for coming. Laura and I are honored to welcome you here.

The Medal of Freedom is the highest civil honor a President can bestow. The award recognizes outstanding individuals who have been leaders in their chosen fields, have led lives of vision and character, and have made especially meritorious contributions to our nation and the world. Today we add the names of six remarkable Americans to that select list.

The story of our first recipient begins in a poor neighborhood in the heart of Detroit. This was an environment where many young people lost themselves to poverty and crime and violence. For a time, young Ben Carson was headed down that same path. Yet through his reliance on faith and family, he turned his life into a sharply different direction. Today Dr. Carson is one of the world's leading neurosurgeons. He is renowned for his successful efforts to separate conjoined twins and his expertise in controlling brain seizures. He has worked to be a motivating influence on young people. He and his wife Candy have started an organization that offers college scholarships to students across America. The child of Detroit who once saw a grim future became a scholar, a healer, and a leader.



Ben would be the first to tell you that his remarkable story would not be possible without the support of a woman who raised him and is at his side today. Some moms are simply forces of nature who never take no for an answer. (Laughter.) I understand. (Laughter.) Ben Carson's mom had a life filled with challenges. She was married at the age of 13, and ultimately was left to raise

her two sons alone. She made their education a high priority. Every week the boys would have to check out library books and write reports on them. She would hand them back with check marks, as though she had reviewed them -- never letting on that she couldn't read them. Even in the toughest times, she always encouraged her children's dreams. She never allowed them to see themselves as victims. She never, ever gave up. We're so thrilled you're here. Sonya Carson, welcome to the White House. (Applause.)

Ben has said that one of his role models is Booker T. Washington, who inspired millions and who was one of the first African American leaders ever to visit this house as a guest of a President. He walked on this very floor a little more than a century ago. Today, Ben Carson follows in his footsteps in more ways than one. He's lived true to the words that was once uttered by this great man: "Character, not circumstances, makes the man." Ben, you demonstrate that character every day -- through the life you lead, the care you provide, and the family that you put at the center of your life. Murray, B.J., and Rhoeyce, I know how proud your dad is of each of you. I'm delighted that you have a chance to see how proud our nation is of him. For his skills as a surgeon, high moral standards, and dedication to helping others, I am proud to bestow the Presidential Medal of Freedom on Dr. Benjamin S. Carson, Sr. (Applause.) The bestowing part will take place a little later, Ben. (Applause.)

Three decades ago, a mysterious and terrifying plague began to take the lives of people across the world. Before this malady even had a name, it had a fierce opponent in Dr. Anthony Fauci. As the Director of the National Institute of Allergy and Infectious Diseases for more than 23 years, Tony Fauci has led the fight against HIV and AIDS. He was also a leading architect and champion of the Emergency Plan for AIDS Relief, which over the past five years has reached millions of people -- preventing HIV infections in infants and easing suffering and bringing dying communities back to life.



The man who would lead the fight against this dreaded disease came from an Italian American family in Brooklyn. Even as a boy, Tony was distinguished by his courage. In a neighborhood full of Brooklyn Dodgers fans -- (laughter) -- he rooted for the Yankees. (Laughter.) Tony earned a full scholarship to Regis High School, a Jesuit school in Manhattan. And he still quotes what he learned from Jesuit teaching: "Precision of thought, economy of expression." And now you know why he never ran for public office. (Laughter.)

Those who know Tony do admit one flaw: sometimes he forgets to stop working. He regularly puts in 80-hour weeks. And from time to time, he's even found notes on his windshield left by coworkers that say things like, "Go home. You're making me feel guilty." (Laughter.) A friend once commented that Tony was so obsessed with work that his wife must be a pretty patient woman. The truth of the matter is, she's very busy herself. Christine Grady is a renowned bioethicist. And together they raised three talented daughters: Jennifer, Meghan, and Allison. And I hope each of you know that for all Tony has accomplished, he considers you to be one of his -- not one of his -- his most important achievement. Your love and support have strengthened him as he works to save lives across the world.

For his determined and aggressive efforts to help others live longer and healthier lives, I'm proud to award the Presidential Medal of Freedom to Dr. Anthony S. Fauci. (Applause.)

When Tom Lantos was 16 years old, Nazi troops occupied his hometown of Budapest. During that bitter occupation, young Tom was active in the resistance. He twice was sent to a Nazi labor camp; both times he escaped. Tom and his wife Annette survived the Holocaust. Others in their family did not.

Their experiences amid Nazi terror shaped the rest of their lives. After they left Hungary and made California their home, Tom put his name on the ballot for a seat in the House of Representatives -- and became the only survivor of the Holocaust ever elected to Congress. One of his early acts was to establish the Congressional Human Rights Council [sic]. Annette served as the Caucus's director. Tom earned the respect from both sides of the aisle, and he rose to become the Chairman of the Foreign Affairs Committee. One colleague put it this way: Tom was at the forefront of virtually every human rights battle over nearly three decades in the Congress.



On Capitol Hill, Tom displayed the energy and enthusiasm of people half his age. When he was in his seventies, he said that he was at the midpoint of his Congressional career. (Laughter.) When he was diagnosed with a fatal form of cancer, he responded with typical grace. As he announced his decision to retire from the job he loved, his words were not of despair, but of gratitude for a nation that had given him so much. Only in America, he said, could a penniless survivor of the Holocaust receive an education, raise a family, and have the privilege of serving in the Congress. That dying servant of the people then said this: "I will never be able to express fully my profoundly felt gratitude to this great country."

America is equally grateful to Tom Lantos. We miss his powerful voice and his strong Hungarian accent. (Laughter.) We miss his generosity of spirit. And we miss his vigorous defense of human rights and his powerful witness for the cause of human freedom. For a lifetime of leadership, for his commitment to liberty, and for his devoted service to his adopted nation, I am proud to award the Presidential Medal of Freedom, posthumously, to Tom Lantos, and proud that his loving wife Annette will receive the award on behalf of his family. (Applause.)

One of my great privileges as the President has been to meet so many outstanding Americans who volunteer to serve our nation in uniform. I've been inspired by their valor, selflessness, and complete integrity. I found all those qualities in abundance in General Peter Pace. As Chairman of the Joint Chiefs of Staff, Pete Pace was a skilled and trusted advisor in a time of war. He helped transform our military into a more efficient and effective force in America's defense.

General Pace experienced the blessings America offers at an early age. He was born in Brooklyn to an Italian immigrant father who sometimes worked two or three jobs at a time to make ends meet. He was raised by a mom who instilled in him the sustaining power of faith. Together his parents raised four children who each went on to great achievements in their chosen fields. That childhood gave young Pete Pace an early glimpse of what he would later call "the incredible benefits that our nation bestows on those who come to our shores."

Pete Pace attended the Naval Academy, and as a young Marine soon found his way to Vietnam. The age of 22, he took command of a platoon engaged in heavy fighting against the enemy during the Tet offensive. Pete quickly won the respect and the trust of his unit and formed a bond with all those who served with him. That bond only strengthened throughout his military career.

He was the first Marine to serve as Chairman of the Joint Chiefs of Staff. And he performed his duties with a keen intellect, a sharp wit, and a passionate devotion to our country. He won the admiration of all who knew him. And that includes a soldier in Afghanistan who came up to General Pace last year during his farewell visit to that country, and said simply: "Sir, thanks for your service. We'll take it from here."

On his final day in uniform, General Pace took a quiet journey to the Vietnam Veterans' Memorial. He searched the names engraved in the sleek granite, and then found a spot where he placed his four stars that had adorned his uniform. Along with those stars he attached notes addressed to the

men who died under his first command some four decades ago. The notes said: "These are yours -- not mine. With love and respect, your platoon leader, Pete Pace." General Pace ended his military career the same way that he began it -- with love for his country and devotion to his fellow Marines.

For his selfless service to his country, and for always putting the interests of our men and women in uniform first, I am proud to award the Presidential Medal of Freedom to General Pete Pace. (Applause.)

When Donna Shalala was 10 years old, a tornado struck her -- struck her house and her neighborhood near Cleveland. Her parents searched throughout the house for young Donna, but couldn't find her anywhere. She was finally spotted down the road, standing in the middle of the road directing traffic. (Laughter.) Even at a young age, she was ready to take charge. (Laughter.)

Donna was always an enthusiastic participant in life. She once played on the girls' softball team coached by George Steinbrenner. (Laughter.) She also joined the Peace Corps and was stationed in the Middle East. I really wonder which one of those two experiences was more challenging. (Laughter.)

In 1993, President Clinton nominated Donna as the nation's Secretary of Health and Human Services. She served for a full two terms -- longer than any other person who held that position. During her tenure, she developed a reputation for fairness, and a willingness to hear both sides of an issue. Former Republican governor who worked closely with Donna called her "cooperative" and "pragmatic." The late Texas columnist Molly Ivins once called her "almost disgustingly cheerful." (Laughter.) I knew Molly -- that's a high compliment. (Laughter.)

As a college president, Donna has demonstrated her commitment to education. And as co-chair of the Dole-Shalala Commission on Care for America's Returning Wounded Warriors, she has worked to ensure that we provide the best possible care for America's veterans, especially those who have borne the scars of battle. I came to know Donna in the course of the Commission's work. She believes deeply that our nation has no more important responsibility than to make sure that we provide our veterans with all the love and care and support they deserve. Donna, you helped America move closer to realizing that noble goal -- and your country is deeply grateful.

For her efforts to help more Americans live lives of purpose and dignity, I am proud to award the Presidential Medal of Freedom to Donna Edna Shalala. (Laughter.)

Few men have played roles in as many memorable moments in recent American history as Laurence Silberman. He was a senior official in the Justice Department in the aftermath of Watergate, and helped to restore America's confidence in the Department. As Ambassador to Yugoslavia, he was a vigorous representative of America's values behind the Iron Curtain. He was a fierce advocate for the "peace through strength" policies that helped win the Cold War.

As a federal judge on the D.C. circuit -- often called the second-highest court in the land -- Judge Silberman has been a passionate defender of judicial restraint. He writes opinions that one colleague has described as always cutting to the heart of the matter -- sometimes to the jugular. (Laughter.) His questioning is crisp and incisive -- and at least one lawyer who was subjected to his inquiries actually fainted. (Laughter.) Judge Silberman was a particularly important influence on two other members of that court: Antonin Scalia and Clarence Thomas. When each was nominated to the Supreme Court, Judge Silberman, in typical fashion, was not sad to see them go. That's because when Scalia left the court, Judge Silberman gained seniority. And when Thomas left the court, Judge Silberman gained his furniture. (Laughter.)

In a new and dangerous era for our country, Larry Silberman has continued to answer the call to service. He served with distinction on the Foreign Intelligence Surveillance Court of Review. He

took a year off from the federal bench to serve as co-chairman of a bipartisan commission on intelligence reform. And in all his work, he's remained a clear-eyed guardian of the Constitution. He continues to leave his distinctive mark in the opinions he issues, and the generations of bright and talented lawyers he has trained.

For his resolute service to the nation and his stalwart efforts to advance the cause of ordered liberty, I am proud to bestow the Presidential Medal of Freedom on Laurence H. Silberman. (Applause.)

My congratulations to each of the recipients. And now the military aide will read the citations for the Presidential Medals of Freedom.

MILITARY AIDE: Dr. Benjamin S. Carson, Sr. (Laughter and applause.) Dr. Benjamin Carson is a pioneer in pediatric neurosurgery, and his life is a testament to the power of education, hard work, and faith. His groundbreaking contributions to medicine provide hope for people suffering neurological disorders, and his tireless outreach to America's youth underscores the importance of academic achievement and humanitarian service. The United States honors Benjamin Carson for his skill, his vision, and his dedication to motivating others to strive for excellence. (Applause.)

(The Medal is presented.) (Applause.)

Anthony S. Fauci, M.D. (Applause.) As a physician, medical researcher, author, and public servant, Dr. Anthony Fauci has dedicated his life to expanding the horizons of human knowledge and making progress toward groundbreaking cures for diseases. His efforts to advance our understanding and treatment of HIV/AIDS have brought hope and healing to tens of millions in both developed and developing nations. The United States honors Anthony Fauci for his commitment to enabling men, women, and children to live longer, healthier lives. (Applause.)

(The Medal is presented.) (Applause.)

Mrs. Annette Lantos, accepting the Medal of Freedom on behalf of her late husband, Tom Lantos. (Applause.) Tom Lantos was a champion of human rights and a man of character and conviction. An American by choice and the only Holocaust survivor to serve in the Congress, he worked to empower oppressed people around the world in their struggle to secure liberty. He served as a powerful witness for the importance of freedom and reminded us that we must never turn a blind eye to inhumanity. The United States honors Tom Lantos for his committed leadership and his lifetime of service to our nation and the world. (Applause.)

(The Medal is presented.) (Applause.)

General Peter Pace, U.S. Marine Corps (Ret.) (Applause.) The 16th Chairman of the Joint Chiefs of Staff, General Peter Pace is one of our nation's most accomplished and respected military leaders. He fought for our nation with honor, and he helped to craft America's response to an unprecedented assault on our homeland. The United States honors Peter Pace for his steadfast leadership, his selfless devotion to keeping Americans safe, and his great courage. (Applause.)

(The Medal is presented.) (Applause.)

Donna Edna Shalala. (Applause.) A distinguished scholar, teacher, academic administrator, and public servant, Donna Shalala has dedicated herself to improving the lives of her fellow citizens. She has devoted her prodigious energies to strengthening a wide range of institutions fundamental to American life. The United States honors Donna Shalala for her leadership and for her determination to ensure that all Americans can enjoy lives of hope, promise, and dignity. (Applause.)

(The Medal is presented.) (Applause.)

Laurence H. Silberman. (Applause.) Laurence H. Silberman has devoted his life to promoting, enforcing, and defending the rule of law. As a judge, he has been a clear-eyed guardian of the Constitution, and he has applied the law with wisdom and integrity. From the Cold War to the war on terror, his work to strengthen the institutions that protect our nation has made Americans safer and their liberties more secure. The United States honors Laurence Silberman for his resolute service to the nation and his stalwart efforts to advance the cause of ordered liberty. (Applause.)

(The Medal is presented.) (Applause.)

THE PRESIDENT: In honor of these distinguished men and women, Laura and I invite you to stay for a reception in the State Dining Room. Please enjoy yourselves. Congratulations. May God bless you all. (Applause.)

END 10:11 A.M. EDT

DEFENDANTS' EXHIBIT 91:

**STATEMENTS & RELEASES**

Statement from the Press Secretary Regarding the President's Coronavirus Task Force

HEALTHCAREIssued on: **January 29, 2020**

Today, President Donald J. Trump announced the formation of the President's Coronavirus Task Force. Members of the Task Force have been meeting on a daily basis since Monday. At today's meeting, which the President chaired, he charged the Task Force with leading the United States Government response to the novel 2019 coronavirus and with keeping him apprised of developments.

The Task Force is led by Secretary of Health and Human Services Alex Azar, and is coordinated through the National Security Council. It is composed of subject matter experts from the White House and several United States Government agencies, and it includes some of the Nation's foremost experts on infectious diseases.

The Task Force will lead the Administration's efforts to monitor, contain, and mitigate the spread of the virus, while ensuring that the American people have the most accurate and up-to-date health and travel information.

The President's top priority is the health and welfare of the American people. That is why, in 2018, President Trump signed the [National Biodefense Strategy](#), which improves speed of action in situations such as this. The Administration, led by the President's Task Force, will continue to work to prevent the spread of the new coronavirus.

The risk of infection for Americans remains low, and all agencies are working aggressively to monitor this continuously evolving situation and to keep the public informed. For more information, please visit [CDC.gov](https://www.cdc.gov).

Members of the President's Coronavirus Task Force:

Secretary Alex Azar, Department of Health and Human Services

Robert O'Brien, Assistant to the President for National Security Affairs

Dr. Robert Redfield, Director of the Centers for Disease Control and Prevention

Dr. Anthony Fauci, Director of the National Institute of Allergy and Infectious Diseases at the National Institutes of Health

Deputy Secretary Stephen Biegun, Department of State

Ken Cuccinelli, Acting Deputy Secretary, Department of Homeland Security

Joel Szabat, Acting Under Secretary for Policy, Department of Transportation

Matthew Pottinger, Assistant to the President and Deputy National Security Advisor

Rob Blair, Assistant to the President and Senior Advisor to the Chief of Staff

Joseph Grogan, Assistant to the President and Director of the Domestic Policy Council

Christopher Liddell, Assistant to the President and Deputy Chief of Staff for Policy Coordination

Derek Kan, Executive Associate Director, Office of Management and Budget



The White House



President Donald J. Trump

Vice President Mike Pence

First Lady Melania Trump

Mrs. Karen Pence

The Cabinet

Administration Accomplishments

News

Remarks

Articles

Presidential Actions

Briefings & Statements

About The White House

Economy & Jobs

Budget & Spending

Education

Immigration

National Security & Defense

Healthcare

Council of Economic Advisers

Council of Environmental Quality

National Security Council

Office of Management and Budget

Office of National Drug Control Policy

Office of Science and Technology Policy

DEFENDANTS' EXHIBIT 92:

AUGUST 22, 2022

Statement from President Joe Biden on the announcement of Dr. Anthony Fauci's Departure from NIAID

During my time as Vice President, I worked closely with Dr. Anthony Fauci on the United States' response to Zika and Ebola. I came to know him as a dedicated public servant, and a steady hand with wisdom and insight honed over decades at the forefront of some of our most dangerous and challenging public health crises. When it came time to build a team to lead our COVID-19 response – in fact, in one of my first calls as President-elect – I immediately asked Dr. Fauci to extend his service as my Chief Medical Advisor to deal with the COVID-19 crisis our nation faced. In that role, I've been able to call him at any hour of the day for his advice as we've tackled this once-in-a-generation pandemic. His commitment to the work is unwavering, and he does it with an unparalleled spirit, energy, and scientific integrity.

Dr. Fauci has served under seven Republican and Democratic Presidents during his career, beginning with Ronald Reagan. He was awarded the Presidential Medal of Freedom in 2008 under President George W. Bush. For almost four decades, he has served as Director of the National Institute of Allergy and Infectious Diseases, helping our country navigate health crises ranging from HIV/AIDS to COVID-19. Because of Dr. Fauci's many contributions to public health, lives here in the United States and around the world have been saved. As he leaves his position in the U.S. Government, I know the American people and the entire world will continue to benefit from Dr. Fauci's expertise in whatever he does next. Whether you've met him personally or not, he has touched all Americans' lives with his work. I extend my deepest thanks for his public service. The United States of America is stronger, more resilient, and healthier because of him.

###

DEFENDANTS' EXHIBIT 93:



Dr. Anthony Fauci to Leave NIAID at the End of December

Funding News Edition: **December 07, 2022**


See more articles in this edition (</grants-contracts/funding-news?edition=2022-12-07>)

At the end of this month, Dr. Anthony Fauci (<https://www.niaid.nih.gov/about/director>), Director of NIAID, will step down from the role he's held since 1984. As he stated in an August 22, 2022 news release (<https://www.niaid.nih.gov/news-events/statement-anthony-s-fauci-md>), "While I am moving on from my current positions, I am not retiring. After more than 50 years of government service, I plan to pursue the next phase of my career while I still have so much energy and passion for my field."

His departure should not prompt any changes to NIAID's extramural funding procedures.

NIH is conducting a nationwide search to find the Institute's next Director. You can read and share the Job Announcement Description (<https://www.niaid.nih.gov/about/niaid-director>).

Contact Us

Email us at deaweb@niaid.nih.gov  for help navigating NIAID's grant and contract policies and procedures.

Stay Connected

- Subscribe to Funding News email updates [✉](http://service.govdelivery.com/accounts/USNIAID/subscriber/new)
(<http://service.govdelivery.com/accounts/USNIAID/subscriber/new>)
- Twitter: @NIAIDFunding [✉](https://twitter.com/NIAIDfunding) (<https://twitter.com/NIAIDfunding>)

Content last reviewed on December 7, 2022

DEFENDANTS' EXHIBIT 94:

Dr. Anthony Fauci's 18-Hour Schedule Is Exhausting to Read

businessinsider.com/dr fauci 18 hour schedule i exhaust ing to read 2020 12

Azmi Haroun



Dr. Anthony Fauci arriving to testify before the House in Washington, DC, on June 23.
Kevin Dietsch/Pool via REUTERS

- In an interview with HuffPost, Dr. Anthony Fauci, the US's leading infectious-disease expert, laid out a schedule of one of his workdays during the COVID-19 pandemic.
- Fauci, who still fits patient visits into his day and is escorted by a team of federal agents because of threats to his safety, mentioned one scheduled 20-minute break within the particular 18-hour workday.
- That day largely revolved around press appearances and emails.
- "I don't socialize," Fauci told HuffPost. "It's my wife and I and the federal agents. We've sort of become like a new family unit "
- Visit Business Insider's homepage for more stories.

Top editors give you the stories you want — delivered right to your inbox each weekday.



By clicking 'Sign up', you agree to receive marketing emails from Insider as well as other partner offers and accept our [Terms of Service](#) and [Privacy Policy](#).

As the COVID-19 pandemic surges, the US's top infectious-disease expert is seemingly everywhere at once.

Dr. Anthony Fauci, the director of the National Institute of Allergy and Infectious Diseases, who turns 80 next week, gave an interview [with HuffPost](#) last week in which he broke down his 18 hour schedule for the day before Thanksgiving. He told HuffPost's Jeffrey Young, who [tweeted out](#) a transcript of Fauci's full answer to his question, that every day was different, and, "It's just, you know, drinking out of a firehose trying to keep ahead of everything that's going on."

- **5:10 a.m. to 6 a.m.:** A shower and a shave.
- **6 a.m. to 6:30 a.m.:** Checking emails. Fauci described receiving more than 1,000 emails, which are whittled down to hundreds of critical ones he must address throughout the day.
- **6:30 a.m. to 7 a.m.:** [Taping a segment](#) for ABC News' "Good Morning America."
- **7 a.m. to 7:30 a.m.:** Leaving home, with a crew of federal agents for protection, to head to the National Institutes of Health.
- **7:30 a.m. to 8 a.m.:** [Appearing on](#) C-SPAN's "Washington Journal."
- **8 a.m. to 8:30 a.m.:** [Calling in to](#) WNYC-FM's "The Takeaway."
- **8:30 a.m. to 9 a.m.:** Taping an interview with a local Chicago TV station.
- **9 a.m. to 10 a.m.:** Checking up on two severe COVID-19 patients at the NIH Clinical Center alongside their primary physicians.
- **10 a.m. to 10:30 a.m.:** Taking part in a videoconference with the National Institute of Allergy and Infectious Diseases staff.
- **10:30 a.m. to 11 a.m.:** Interview with a newspaper reporter.
- **11 a.m. to 11:50 a.m.:** Video meeting with HHS Secretary Alex Azar, NIH Director Francis Collins, CDC Director Robert Redfield, FDA Administrator Stephen Hahn, and others.
- **11:50 a.m. to noon:** A "10-12 min" bathroom break and emails.
- **Noon to 12:30 p.m.:** [Interview with theGrio](#) about vaccine skepticism in the Black community.
- **12:30 p.m. to 1 p.m.:** HuffPost's [interview](#).
- **1 p.m. to 1:30 p.m.:** More TV appearances.
- **1:30 p.m. to 1:50 p.m.:** The first true break scheduled that day.
- **1:50 p.m. to 2:30 p.m.:** A newspaper interview.
- **2:30 p.m. to 3 p.m.:** An interview with a scientific journal.
- **3 p.m. to 3:30 p.m.:** Preparing "for an upcoming speech to the Centers for Science and International something-or-other, one of those think tanks in Washington."
- **3:30 p.m. to 4:30 p.m.:** Videoconference with doctors from the White House coronavirus task force.

- **4:30 p.m. to 5:30 p.m.:** Videoconference with NIH vaccine scientists, including Moderna and other producers
- **5:30 p.m. to 7 p.m.:** Phone calls, emails, and more press.

After his arduous schedule, Fauci said he hoped to be home after 7 p.m., where he would finish off the day doing his 45 minute power walk with his wife, Christine Grady, the chief of the Department of Bioethics at the NIH's Clinical Center.

After dinner, he would do more press and check more emails until he said he's "so tired I can't do anymore."

In his interview with HuffPost, Fauci also mentioned that because of COVID-19 and threats made against his life (including a comment by the former Trump White House chief strategist Steve Bannon calling for Fauci's head on a pike), he does not socialize and did not hold any Thanksgiving gatherings with his children

"I have federal agents that protect me. So they drive me to work, they stay here, they make sure that nobody tries to break in [to my home] and, as Steve Bannon would like, have somebody behead me," Fauci told HuffPost. "I don't socialize. It's my wife and I and the federal agents. We've sort of become like a new family unit."

As vaccines become accessible to the mass public and until the pandemic seriously subsides in the US, Fauci is expecting to be busy, especially as President-elect Vice Biden said Thursday that he planned to keep Fauci in his current position, as well as a chief medical advisor, after taking office.



Sign up for notifications from Insider! Stay up to date with what you want to know.

Subscribe to push notifications

Read next

NOW WATCH: 5 times Trump praised Dr. Fauci prior to retweeting that he should be fired

DEFENDANTS' EXHIBIT 95:



NATIONAL ACADEMY OF SCIENCES



ABOUT THE NAS

MEMBERSHIP

PROGRAMS

PUBLICATIONS

MEMBER LOGIN



Programs

Awards

2021 Awards

Anthony S. Fauci

+ Share

PROGRAMS

Awards

- » 2023 Awards
- » 2024 Awards
- » How to Nominate
- » Alphabetical Listing
- » Awards by Field
- » Award Lectures
- » Looking Forward
- » The Science Explained
- » Connect with Awards

Cultural Programs

Distinctive Voices

Human Gene Editing Initiative

Kavli Frontiers of Science

LabX

US-UK Scientific Forum

Blavatnik US-Israel Scientific Forum

From Research to Reward

The Science Behind It

Science & Entertainment Exchange

Engagement Opportunities
Committee on International
Security and Arms Control

Committee on Human Rights

Committee on Science,
Engineering, Medicine, and
Public PolicyCommittee on Women in
Science, Engineering and
MedicineGovernment-University-
Industry Research Roundtable

NAS Colloquia (inactive)



Scientist, physician, and public health leader **Anthony S. Fauci** received the 2021 **NAS Public Welfare Medal** for his “decades-long leadership in combatting emerging infectious diseases, from the AIDS crisis to the COVID-19 pandemic, and being a clear, consistent, and trusted voice in public health.” The medal is the Academy’s most prestigious award, established in 1914 and presented annually to honor extraordinary use of science for the public good.

Fauci’s career as a public servant spans more than four decades, and he has advised seven U.S. presidents, including President Joe Biden. The director of the National Institute of Allergy and Infectious Diseases (NIAID) at the National Institutes of Health, Fauci has played a key role in shaping the federal government’s response to the COVID-19 pandemic while leading NIAID-sponsored research efforts to better understand, prevent, and treat COVID-19. Despite a heavy workload, he continues to promote and reinforce critical public health guidance through numerous media appearances, clearly and compellingly informing the public based on the best available science and evidence – all while directing the NIAID research enterprise, treating patients and conducting research in his own laboratory.

“During this extraordinarily challenging time for the nation and the world, Anthony Fauci has never wavered, tirelessly working almost around the clock to help America fight COVID-19,” said Susan Wessler, Home Secretary of the National Academy of Sciences and Chair of the selection committee for the award. “He is an outstanding physician, researcher, and public servant whose immeasurable contributions to public health and welfare have undoubtedly made all of our lives better.”

“Anthony Fauci is an American hero who has earned the respect and trust of millions for his no-nonsense approach to the pandemic,” said National Academy of Sciences President Marcia McNutt. “Throughout his long and distinguished career, his leadership and ingenuity during public health emergencies has saved countless lives here in the U.S. and around the world. I am delighted to present him with the Academy’s most prestigious award.”

Long before he became a household name for his work on the COVID-19 pandemic, Fauci was a pioneer in the prevention, diagnosis, and treatment of infectious diseases, helping to steer the nation and the world through many public health crises, including HIV/AIDS, Ebola, the swine flu, and Zika. Fauci was also the principal architect of the President’s Emergency Plan for AIDS Relief (PEPFAR), a lifesaving global program that has accelerated progress toward controlling the HIV/AIDS epidemic in more than 50 countries. In recognition of his leadership in PEPFAR, President George W. Bush awarded him the Medal of Freedom, the nation’s highest civilian honor. Fauci also contributed to the establishment of the U.S. President’s Malaria Initiative in 2005, a program that has greatly reduced the burden of this disease in Africa and Asia.

Fauci has made seminal contributions to the understanding of how HIV destroys the body’s defenses leading to its susceptibility to deadly infections, and in developing treatments that enable people with HIV to live long and active lives. He continues to devote much of his research to the immunopathogenic mechanisms of HIV infection and the scope of the body’s immune responses to HIV. As the longtime chief of the Laboratory of Immunoregulation, Fauci also developed effective therapies for once fatal inflammatory and immune-mediated diseases.

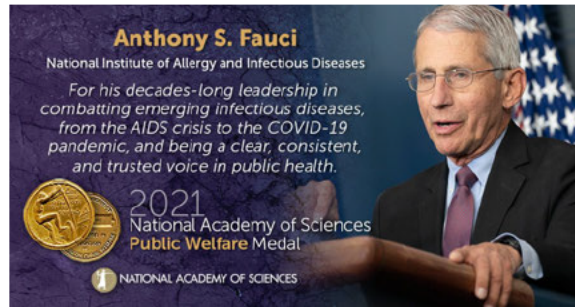
In addition to the Presidential Medal of Freedom, Fauci has received numerous other awards and honors. He is a recipient of the National Medal of Science, the George M. Kober Medal of the Association of American Physicians, the Mary Woodard Lasker Award for Public Service, the Albany Medical Center Prize in Medicine and Biomedical Research, the Robert Koch Gold Medal, the Prince Mahidol Award, and the Canada Gairdner Global Health Award. He is a member of the National Academy of Sciences, the National Academy of Medicine, the American Academy of Arts and Sciences, and the American Philosophical Society, as well as other professional societies; has received 45 honorary doctoral degrees from universities in the United States and abroad; and is the author, co-author, or editor of more than 1,300 scientific publications, including several textbooks.

The Public Welfare Medal will be presented to Anthony Fauci during the Academy’s 158th annual meeting.

The NAS Public Welfare Medal is the Academy’s most prestigious award, established in 1914 and presented annually to honor

National Academies Keck
Futures Initiative (inactive)

extraordinary use of science for the public good.



Links

[Press Release »](#)

[Public Welfare Medal »](#)

[2021 NAS Award Recipients »](#)

National Academy of Sciences

ABOUT THE NAS

[Mission](#)

[History](#)

[Organization](#)

[Leadership and Governance](#)

[Membership](#)

[Policy Studies and Reports](#)

[Giving to NAS](#)

ACTIVITIES & PROGRAMS

[Awards](#)

[Cultural Programs](#)

[Distinctive Voices Lecture Series](#)

[Human Gene Editing Initiative](#)

[Kavli Frontiers of Science Symposia](#)

[LabX](#)

[US-UK Scientific Forum](#)

[Blavatnik US-Israel Scientific Forum](#)

[From Research to Reward](#)

[The Science Behind It](#)

[Science & Entertainment Exchange](#)

[Committee on International Security and Arms Control](#)

[Committee on Human Rights](#)

[Committee on Science, Engineering, Medicine, and Public Policy](#)

[Committee on Women in Science, Engineering, and Medicine](#)

[Government-University-Industry Research Roundtable](#)

PUBLICATIONS

[Proceedings \(PNAS\)](#)

[PNAS Nexus](#)

[National Academies Press](#)

[Biographical Memoirs](#)

[Issues in Science and Technology](#)

RESOURCES

[Newsroom](#)

[Member Directory](#)

[Meetings & Events](#)

[Locations](#)

[Careers](#)

[Directory](#) | [Meetings & Events](#) | [Support the NAS](#)



Copyright © 2023 National Academy of Sciences. All rights reserved.
Terms of Use and Privacy Policy

NATIONAL ACADEMIES
Sciences
Engineering
Medicine

DEFENDANTS' EXHIBIT 96:



Anthony Fauci Named Recipient of AHA Award of Honor

🏠 (/) / [Press \(/taxonomy/term/120\)](#) / [Press Releases \(/press-release\)](#)

WASHINGTON (April 21, 2022) – The American Hospital Association (AHA) today announced that its 2021 Award of Honor will be presented to the National Institute of Allergy and Infectious Diseases (NIAID) Director Anthony S. Fauci, M.D., for his tireless efforts to educate and counsel health care providers and the public during the COVID-19 pandemic. The award is given to individuals or organizations in recognition of exemplary contributions to the health and well-being of our nation through leadership on major health policy or social initiatives. Dr. Fauci will receive the award during a ceremony on April 25 at the AHA Annual Membership Meeting in Washington, D.C.

When Dr. Fauci joined the White House Coronavirus Task Force in January 2020, the impending breadth and depth of the virus's toll, plus the politicization of science and medicine, were still unknown. As cases of COVID-19 began to surge throughout the country, Dr. Fauci advised the administration, the health care field and the public about the evolving science of COVID-19 and how to slow its spread.

"Serving as a trusted and calming voice on COVID-19 for the nation, Dr. Fauci was relentless advising the government, the health care field and the public on ways to battle the pandemic," said Rick Pollack, AHA president and CEO. "His expertise, courage and grit guided our nation through some of our darkest days. We're honored to recognize his lifetime dedication to service and commitment to enhancing public health."

Appointed as NIAID director in 1984, Dr. Fauci oversees an extensive research portfolio of basic and applied research to prevent, diagnose, and treat established infectious diseases such as HIV/AIDS, respiratory infections, diarrheal diseases, tuberculosis and malaria as well as emerging diseases such as COVID-19, Ebola and Zika. During his tenure as NIAID director, he has advised seven presidents on many domestic and global health issues.

###

Contact: Marie Johnson, mjohnson@aha.org (<mailto:mjohnson@aha.org>)
Colin Milligan, cmilligan@aha.org (<mailto:cmilligan@aha.org>)

About the American Hospital Association

The American Hospital Association (AHA) is a not-for-profit association of health care provider organizations and individuals that are committed to the health improvement of their communities. The AHA advocates on behalf of our nearly 5,000 member hospitals, health systems and other health care organizations, our clinician partners – including more than 270,000 affiliated physicians, 2 million nurses and other caregivers – and the 43,000 health care leaders who belong to our professional membership groups. Founded in 1898, the AHA provides insight and education for health care leaders and is a source of information on health care issues and trends. For more information, visit the AHA website at www.aha.org (<http://www.aha.org>).

Related Resources

AWARD

About Foster G. McGaw (/award/2023-03-22-about-foster-g-mcgaw)

ADVANCING HEALTH PODCAST

#JustLead featuring Cheshire Medical Center (/advancing-health-podcast/2022-11-16-justlead-featuring-cheshire-medical-center)

ADVANCING HEALTH PODCAST

#JustLead featuring Salinas Valley Memorial Health and Montage Health (/advancing-health-podcast/2022-10-28-justlead-featuring-salinas-valley-memorial-health-and-montage-health)

ADVANCING HEALTH PODCAST

#JustLead featuring NorthShore University HealthSystem (/advancing-health-podcast/2022-10-19-justlead-featuring-northshore-university-healthsystem)

ADVANCING HEALTH PODCAST

#JustLead Featuring WellSpan Health (/advancing-health-podcast/2022-10-14-justlead-featuring-wellspan-health)

ADVANCING HEALTH PODCAST

#JustLead featuring University Hospitals (/advancing-health-podcast/2022-09-16-justlead-featuring-university-hospitals)

RELATED TOPICS: Recognition and Awards (/topics/recognition-and-awards)

RELATED

News Articles

AHA honors federal health care leaders (/news/headline/2023-04-24-aha-honors-federal-health-care-)	Texas health system to receive 2023 Foster G. McGaw Prize (/news/headline/2023-04-21-texas-health-system-)	Skogsbergh to receive AHA Distinguished Service Award (/news/headline/2023-04-19-skogsbergh-)	Pelosi to receive AHA Award of Honor (/news/headline/2023-04-18-pelosi-receive-aha-award-honor)	Health system leader to receive AHA Justin Ford Kimball Innovators Award (/news/headline/2023-04-17-health-)	AHA announces 2023 AHA Honorary Life Membership Award recipient (/news/headline/2023-04-14-aha-)
--	--	---	---	--	--

RELATED

Events & Education

Health Care Strategy & Market Development Week (https://www.shsmd.org/node/385362) Nov 13, 2022 -	Equity of Care Awards Informational Session (/education-2022-10-26-21-aha-nova-awards-webinar) Oct 26, 2020 -	Profiles in Excellence: Northside Hospital (https://www.aha.org/node/692792) Jun 22, 2022 - 09:00 PM	AHA NOVA Awards Webinar Oct 26 (/education-2022-10-26-21-aha-nova-awards-webinar) Oct 26, 2020 -	National Health Care Supply Chain Week (https://www.ahmm.org/node/382470) Oct 04, 2020 - 12:00 AM - Oct 10, 2020 - 11:59 PM
--	--	---	--	--



(/)

Advancing Health in America

[ABOUT AHA \(/ABOUT\)](#)

[ADVOCACY \(/ADVOCACY/2020-01-30-2020-AHA-ADVOCACY-AGENDA\)](#)

[CAREER RESOURCES \(/ABOUT/CAREERS-AHA\)](#)

[DATA & INSIGHTS \(/DATA-INSIGHTS/HEALTH-CARE-BIG-PICTURE\)](#)

[EDUCATION AND EVENTS \(/CALENDAR\)](#)

[NEWS \(/NEWS\)](#)

[ADVANCING HEALTH IN AMERICA \(/ADVANCING-HEALTH-IN-AMERICA\)](#)

[PRESS CENTER \(/PRESS-CENTER\)](#)

[AFFILIATED ORGANIZATIONS \(/ABOUT/AHA-RELATED-ORGANIZATIONS\)](#)

ALSO OF INTEREST

[Multidisciplinary CAUTI Prevention Team \(https://www.aha.org/websites/2016-02-29-cauti-prevention-team\)](https://www.aha.org/websites/2016-02-29-cauti-prevention-team)

[Health Care for the Homeless \(https://www.aha.org/websites/2016-02-29-health-care-homeless\)](https://www.aha.org/websites/2016-02-29-health-care-homeless)

[Workforce \(https://www.aha.org/workforce-home\)](https://www.aha.org/workforce-home)

© 2023 by the American Hospital Association. All rights reserved. [Privacy Policy \(/2022-07-14-privacy-policy\)](#) [Terms of Use \(/2022-07-14-termsofuse\)](#)

[f \(https://www.facebook.com/ahahospitals\)](https://www.facebook.com/ahahospitals) [t \(http://twitter.com/ahahospitals\)](http://twitter.com/ahahospitals) [v \(http://www.youtube.com/user/AHAhospitals\)](http://www.youtube.com/user/AHAhospitals)
[i \(https://www.instagram.com/ahahospitals/\)](https://www.instagram.com/ahahospitals/)

Noncommercial use of original content on www.aha.org is granted to AHA Institutional Members, their employees and State, Regional and Metro Hospital Associations unless otherwise indicated. AHA does not claim ownership of any content, including content incorporated by permission into AHA produced materials, created by any third party and cannot grant permission to use, distribute or otherwise reproduce such third party content. To request permission to reproduce AHA content, please click here (<https://askrc.libraryresearch.info/ref100.aspx?key=ExtPerm>).

DEFENDANTS' EXHIBIT 97:

**IN THE UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF LOUISIANA**

The State of Missouri, *et al.*,

Plaintiffs,

v.

President Joseph R. Biden, Jr., in his official
capacity as President of the United States of
America, *et al.*,

Defendants.

Civil Action No. 22-cv-1213

DECLARATION OF GEOFF HALE

I, Geoff Hale, declare the following, based upon my personal knowledge, information acquired by me in the course of performing my official duties, and information contained in the records of the Cybersecurity and Infrastructure Security Agency (CISA):

1. I am the Lead for Election Security and Resilience within the National Risk Management Center at CISA, U.S. Department of Homeland Security (DHS). I joined the Department in 2015, and I have supported the Department's and Agency's election security mission since 2016. I am responsible for leading CISA's Election Security and Resilience team, which includes the Mis-, Dis-, and Malinformation (MDM) team.

I. CISA's Mission

2. As the nation's cyber defense agency, CISA is charged with leading the national effort to understand, manage, and reduce risk to the nation's cyber and physical infrastructure. 6 U.S.C. § 652. Securing the nation's critical infrastructure is a shared responsibility requiring not just a whole-of-government, but a whole-of-nation approach. CISA is only able to accomplish its

mission by building collaborative, trusted partnerships across all levels and branches of government, and with the private sector, academia, and international community.

3. As part of this mission, CISA plays two key operational roles. First, CISA is the operational lead for federal cybersecurity, in close partnership with federal partners. Second, CISA serves as the National Coordinator for critical infrastructure security and resilience, including cybersecurity, working with partners across government and industry to protect and defend the nation's critical infrastructure.¹

4. In January 2017, the U.S. Department of Homeland Security officially designated election infrastructure as a subsector of the Government Facilities Sector, described below, making clear that election infrastructure qualifies as critical infrastructure. This designation recognizes that U.S. election infrastructure is of such vital importance that its disruption would have a devastating effect on the country.

5. Election infrastructure refers to an assembly of systems and networks, including, among other things, voter registration databases and associated IT systems, IT infrastructure and systems used to manage elections, voting systems and associated infrastructure, storage facilities for election and voting system infrastructure, and polling places. <https://www.cisa.gov/topics/election-security> (last visited April 24, 2023).

6. To manage risks to the nation's election infrastructure, CISA works collaboratively with state and local governments, election officials, federal partners, and private sector partners. The collaboration includes working in a nonpartisan manner with state and local election officials across the political spectrum—including, as discussed below, officials from Louisiana and

¹ 42 U.S.C. § 5195c defines critical infrastructure as “systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.”

Missouri—as the trusted and expert voices within their communities, to hold secure elections in their jurisdictions and to equip the American public with accurate information about the conduct and security of elections.

7. CISA provides publicly available resources on election security for both the general public and election officials in its efforts to protect America’s election infrastructure against new and evolving threats. For example, CISA has publicly released an Election Infrastructure Insider Threat Mitigation Guide (https://www.cisa.gov/sites/default/files/2022-11/election_insider_threat_mitigation_guide_508_0.pdf) (last visited April 24, 2023)); CISA partnered with the Federal Bureau of Investigation (FBI) to publish election-security related public service announcements or PSAs for the general public (*see, e.g.,* FBI & CISA Public Service Announcement, *Malicious Cyber Activity Against Election Infrastructure Unlikely to Disrupt or Prevent Voting* (Oct. 4, 2022), available at <https://www.cisa.gov/resources-tools/resources/psa-malicious-cyber-activity-against-election-infrastructure-unlikely> (last visited April 24, 2023)), and through its Joint Cyber Defense Collaborative, CISA compiled a toolkit of free services and tools intended to help state and local government officials, election officials, and vendors enhance the cybersecurity and cyber resilience of U.S. election infrastructure (*see* <https://www.cisa.gov/cybersecurity-toolkit-and-resources-protect-elections> (last visited April 24, 2023)).

8. CISA also provides numerous voluntary and no-cost election security services, such as cybersecurity assessments, cyber threat hunting, cyber incident response, training and exercises, to state and local government officials and private sector election infrastructure partners. <https://www.cisa.gov/election-security-services> (last visited April 24, 2023).

9. In addition, CISA reduces risk to U.S. critical infrastructure by building resilience to disinformation² related to critical infrastructure. Through these efforts, CISA helps the American people understand the scope and scale of activities targeting election infrastructure and enables them to take action to mitigate associated risks. Sharing accurate and transparent information about election infrastructure, as well as increasing awareness about disinformation, better equips the American people to understand elections and to discern rumors from reality.

10. CISA's disinformation-related work, which is focused on resilience, is actor agnostic, and, thus, CISA does not assess the source of disinformation (*i.e.*, whether it is foreign or domestic).

II. CISA's MDM Team

11. CISA's MDM team works to build national resilience to disinformation and foreign influence operations. Through these efforts, CISA helps the American people understand the scope and scale of disinformation activities targeting election and other critical infrastructure, and enables them to take action to mitigate associated risks. The MDM team was formerly known as the Countering Foreign Influence Task Force (CFITF) and was founded in May of 2018.

12. While CISA anticipated and publicly stated that the MDM Team would grow, the size of the team supporting this mission generally has remained constant.

13. The primary focus and mission of CISA's disinformation-related work has been and continues to be building resilience to disinformation generally and specifically to that affecting election infrastructure. Despite statements to the contrary, the scope of the mission has not expanded, nor have CISA's efforts to build resilience to disinformation. CISA's current efforts to build resilience to disinformation are discussed below.

² In this declaration, I refer to disinformation generally, and I am not differentiating between misinformation, disinformation or malinformation.

14. First, CISA has developed innovative methods to help individuals recognize and avoid disinformation operations. This includes the creation of graphic novels illustrating disinformation tactics through fictional stories and the War on Pineapple infographic designed to explain foreign influence campaigns. See <https://www.cisa.gov/topics/election-security/foreign-influence-operations-and-disinformation/resilience-series-graphic-novels> (last visited April 24, 2023); <https://www.cisa.gov/resources-tools/resources/war-pineapple> (last visited April 24, 2023). CISA has released guides that highlight tactics used by disinformation campaigns, such as manipulating content service providers or defacing public websites, that seek to negatively impact U.S. critical infrastructure and disrupt American life. See, e.g., <https://www.cisa.gov/resources-tools/resources/tactics-disinformation> (last visited April 24, 2023). Such public products help Americans understand how automated programs like social media bots simulate human behavior on social media platforms and how foreign malign actors use them to spread false or misleading information, shut down opposition, and elevate their own platforms for further manipulation.

15. Second, CISA seeks to build resilience to disinformation by providing accurate information in response to inaccurate election security-related information and amplifying accurate information shared by state and local officials with the public. For example, CISA's Election Security Rumor vs. Reality website provides context to common disinformation narratives and themes that relate to the security of election infrastructure (<https://www.cisa.gov/rumor-vs-reality> (last visited April 24, 2023)), and CISA amplifies messaging from state and local election officials through CISA's social media platforms.

16. Third, over the past few years, CISA has also done a limited amount of disinformation-related work concerning other critical infrastructure sectors. None of that work

has involved CISA communicating with social media companies concerning content on their platforms.

17. For example, during the COVID-19 pandemic and in relation to the Healthcare and Public Health Sector, CISA provided support to the sector and produced two public guidance documents: (1) CISA Insights: COVID Disinformation Activity, https://www.cisa.gov/sites/default/files/publications/CISAInsights-COVID-19_Disinformation_Activity_508.pdf (last visited April 24, 2023); and (2) a COVID-19 Toolkit, https://www.cisa.gov/sites/default/files/publications/SLTTCOVIDToolkit_FINAL_508.pdf (last visited April 24, 2023).

18. In support of the President's Unified Coordination Group (UCG) for domestic preparedness and response regarding any potential impacts of Russia's invasion of Ukraine on the United States, which was led by DHS, CISA personnel provided the UCG with situational awareness reports based on publicly available third-party reporting and support to build resilience to disinformation related to the crisis for the purpose of being prepared should foreign influence operations increase its targeting of U.S. critical infrastructure. The UCG was in operation from January 2022 to April 2022.

19. In relation to the Financial Services Sector, CISA has been working with the U.S. Department of Treasury on a guide that would be publicly available to help the Financial Services Sector understand what disinformation is, how disinformation could impact the sector, and how to mitigate the risks to the sector. The guide is still in development, but work is not currently being done to complete it because other tasks have taken priority.

III. Critical Infrastructure Sectors and Related Councils

20. As established by Presidential Policy Directive (PPD) 21,³ there are currently 16 critical infrastructure sectors into which the “systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters” are organized. <https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil/> (last visited April 24, 2023).

21. PPD 21 designates a Sector Risk Management Agency (SRMA) for each sector given that agency’s specialized knowledge and expertise with respect to the sector. *See* 6 U.S.C. § 652a(c)(3) (stating that any reference to a “Sector-Specific Agency” in any document of the United States shall be deemed to be a reference to an SRMA).⁴

22. The Government Facilities Sector helps organize the owners and operators of federal and state, local, tribal and territorial (SLTT) facilities to identify their unique critical infrastructure security and resilience risk factors, share information, and develop best practices to protect against potential attacks on or issues with critical infrastructure. CISA and the General Services Administration serve as co-SRMAs for the Government Facilities Sector.

³ Presidential directives, such as proclamations and executive orders, are used to announce official policy and make declarations by the President. National security directives are a topical subset of presidential directives, and recent presidents have used different names for such directives. The Obama Administration identified national security directives as PPDs, while the George W. Bush Administration called them National Security Presidential Directives and the Trump Administration called them National Security Presidential Memoranda. *See Presidential Directives: An Introduction*, Congressional Research Service (Nov. 13, 2019), available at <https://crsreports.congress.gov/product/pdf/IF/IF11358> (last visited April 24, 2023).

⁴ SRMA means the federal department or agency designated by law or presidential directive, here PPD 21, “with responsibility for providing institutional knowledge and specialized expertise of a sector, as well as leading, facilitating, or supporting programs and associated activities of its designated critical infrastructure sector in the all hazards environment in coordination with the [DHS].” 6 U.S.C. § 651(5).

23. The Election Infrastructure Subsector, a subsector of the Government Facilities Sector, covers a wide range of systems and assets used to support the election process; such as storage facilities, polling places, centralized vote tabulation locations, and information and communications technologies to include voter registration databases, voting machines, and other systems to manage the election process, and report and display election results on behalf of state and local governments. <https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical> (last visited April 24, 2023).

24. Under the National Infrastructure Protection Plan Framework, critical infrastructure sectors and some subsectors are represented by government coordinating councils (GCC) and sector coordinating councils (SCC), along with other information sharing structures. <https://www.cisa.gov/resources-tools/groups/critical-infrastructure-partnership-advisory-council-cipac> (last visited April 24, 2023).

25. GCCs enable members to interact on a wide range of sector-specific strategies, policies, and activities. GCCs are comprised of federal and SLTT governments. <https://www.cisa.gov/resources-tools/groups/government-coordinating-councils> (last visited April 24, 2023).

26. SCCs are self-organized and self-governed councils comprised of critical infrastructure owners and operators, their trade associations, and other industry representatives. <https://www.cisa.gov/resources-tools/groups/sector-coordinating-councils> (last visited April 24, 2023).

27. The Election Infrastructure Subsector is supported by the Election Infrastructure Subsector GCC (EIS-GCC) and the Election Infrastructure SCC (EI-SCC).

28. The EIS-GCC enables state, local, and federal government departments and agencies to share information and collaborate on best practices to mitigate and counter threats to election infrastructure. In particular, the EIS-GCC provides for interagency, intergovernmental, and cross-jurisdictional coordination within the Election Infrastructure Subsector and between this subsector and other sectors.

29. The EIS-GCC is comprised of members from across various levels of government to represent the operating landscape of the Election Infrastructure Subsector, including voting members, non-voting members, alternate representatives, and an executive committee.

30. The EIS-GCC Executive Committee is chaired by CISA, as the Sector Risk Management Agency, and members include the U.S. Election Assistance Commission Chairperson, the National Association of Secretaries of State (NASS) President, the National Association of State Election Directors (NASSED) President, and a local government election official.

31. The Louisiana Secretary of State has been a member of the EIS-GCC since May 2018, and while serving as the NASS President from the summer of 2021 to 2022, the Louisiana Secretary of State served as an EIS-GCC Executive Committee member. In this capacity, Louisiana received regular briefings (usually every two weeks) on CISA's election security efforts, including briefings on CISA's disinformation resilience work, engaged in security planning activities for the Election Infrastructure Subsector, and oversaw the management and activity of EIS-GCC working groups—including the EI-SCC and EIS-GCC Joint Managing Mis/Disinformation Working Group.

32. The Missouri Secretary of State served as an alternate member of the EIS-GCC from 2018 to 2019. In this capacity, Missouri attended the EIS-GCC biannual meetings and

actively participated in briefings on the Election Infrastructure Subsector's security and resilience efforts.

33. In addition, I understand Louisiana is a member of NASS, and Louisiana and Missouri are both members of NASED. *See* <https://www.nass.org/membership> (last visited April 24, 2023); <https://www.nased.org/members> (last visited April 24, 2023).

34. The EI-SCC's mission is "to advance the physical security, cyber security, and emergency preparedness of the nation's election infrastructure," and it is accomplished through voluntary actions of the infrastructure owners and operators represented in the EI-SCC. Membership is available to any owner or operator with significant business or operating interests in U.S. election infrastructure systems or services, including, for example, the technology company Microsoft Corp., because, among other reasons, many voting systems are built on Microsoft operating systems and it provides cybersecurity services used by the election community.

35. The EI-SCC is governed by a five-member Executive Committee.

36. While CISA is not a member of the EI-SCC, it serves as the secretariat and provides various administrative functions.

37. Both the EI-SCC and EIS-GCC have the authority to establish working groups as necessary.

38. After the 2020 election, the EI-SCC and EIS-GCC launched a Joint Managing Mis/Disinformation Working Group to leverage opportunities to coordinate efforts across the subsector. *See* https://www.cisa.gov/sites/default/files/2023-01/ei-ssp-2022-status-update_508.pdf (last visited April 24, 2023).

39. It provides a forum through which the Election Infrastructure Subsector can identify challenges in mitigating the risks posed by disinformation impacting election infrastructure and to produce resources for addressing these risks. *Id.*

40. To date, the EI-SCC and EIS-GCC Joint Managing Mis/Disinformation Working Group has published two guides to help state and local election officials and industry providers prepare for and respond to risks of disinformation: (1) the Rumor Control Page Start-Up Guide, which is designed for use by SLTT government officials and private sector partners seeking to dispel inaccurate election security-related information by sharing accurate information, *see* <https://www.cisa.gov/resources-tools/resources/rumor-control-webpage-start-guide> (last visited April 24, 2023); and (2) the MDM Planning and Incident Response Guide for Election Officials, which is designed for SLTT election officials to help them understand, prepare for, and respond to disinformation that may impact the ability to securely conduct elections, <https://www.cisa.gov/resources-tools/resources/mis-dis-malinformation-planning-and-incident-response-guide-election> (last visited April 24, 2023).

41. Through CISA's roles with the EI-SCC and EIS-GCC, CISA supports the EI-SCC and EIS-GCC Joint Managing Mis/Disinformation Working Group by providing administrative and substantive support, such as facilitating working group meetings and helping to draft working group products.

42. Microsoft, as a member of the EI-SCC, has participated in the Working Group.

43. The Joint Managing Mis/Disinformation Working Group does not engage with social media companies, and it does not flag or report potential disinformation to social media or technology companies.

IV. Center for Internet Security

44. The Center for Internet Security (CIS), a nonprofit, is home to the Multi-State Information Sharing and Analysis Center (MS-ISAC) and the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC). <https://www.cisecurity.org/about-us> (last visited April 24, 2023). CIS, the MS-ISAC, and the EI-ISAC are not government organizations.

45. The MS-ISAC serves as a central cybersecurity resource for U.S. SLTT government entities. It is a membership-based collaborative that is open to SLTT entities of all types, including, but not limited to, SLTT government agencies, law enforcement, educational institutions, public utilities and transportation authorities. <https://www.cisa.gov/resources-tools/services/multi-state-information-sharing-and-analysis-center> (last visited April 24, 2023).

46. MS-ISAC membership includes more than 14,000 organizations and all 50 states are represented, including Missouri and Louisiana. <https://www.cisecurity.org/insights/blog/the-ms-isac-is-now-more-than-14k-members-strong> (last visited April 24, 2023).

47. MS-ISAC provides to its members direct access to a suite of cybersecurity services and cybersecurity informational products including, but not limited to, cybersecurity advisories and alerts, vulnerability assessments, incident response support, secure information sharing, tabletop exercises, and malicious domains/internet protocol reports. <https://www.cisa.gov/resources-tools/services/multi-state-information-sharing-and-analysis-center> (last visited April 24, 2023).

48. Founded in 2018, the EI-ISAC is a voluntary organization managed by CIS with membership open to SLTT organizations and private sector entities that support election officials. The EI-ISAC supports the rapidly changing cyber and critical infrastructure security needs of U.S. elections offices and offers a suite of elections-focused cyber defense tools, including cyber threat intelligence products, incident response and forensics, threat and vulnerability monitoring, and

cybersecurity awareness and training products. <https://www.cisa.gov/resources-tools/groups/join-ei-isac> (last visited April 24, 2023).

49. Membership in the EI-ISAC is voluntary and free for participants. *Id.*

50. DHS has provided financial assistance to CIS through a series of cooperative agreement awards, managed by CISA, to provide certain, specified cybersecurity services to SLTT government organizations through the MS- and EI-ISACs. In the approved scope of work for the cooperative agreements, DHS has limited the use of federal funds and any required non-federal cost-share to cybersecurity services intended to detect, prevent, respond to, mitigate, and recover from cyber threats, vulnerabilities, and risks. DHS has provided financial assistance to CIS through cooperative agreement awards since 2010 to provide such cybersecurity services to SLTT government organizations.

51. The DHS approved scope of work for the cooperative agreements has never funded CIS to perform disinformation-related work, including the reporting of potential election security-related disinformation to social media platforms.

V. Election Integrity Partnership

52. I understand that the Election Integrity Partnership (EIP) is a private partnership formed in 2020 that included the Stanford Internet Observatory (SIO), the University of Washington, Graphika, and the Atlantic Council's Digital Forensic Research Lab to better understand the information environment around elections. *See* Scully Dep. Ex. 1 (The Long Fuse: Misinformation and the 2020 Election at vi). As discussed below, CISA's involvement in the creation and operation of the EIP has been very limited, and CISA did not found, fund, or have any role in the management or operations of the EIP.

53. During 2020, several Stanford University students interned at CISA and worked on election security matters. During their internship, CISA personnel and the interns discussed the

challenges facing and the needs of election officials. Recognizing that state and local election officials often have very limited resources, CISA personnel and the interns discussed that many election officials did not have the resources or capability to identify and respond to potential election security-related disinformation impacting their jurisdictions.

54. I understand that some of the Stanford students who interned at CISA independently made a presentation about this lack of resources and resulting challenge facing election officials to the SIO. Subsequently, CISA personnel had a conversation with SIO personnel during which CISA confirmed that it perceived that state and local election officials lacked the resources and capability to identify and respond to potential election security-related disinformation impacting their jurisdictions.

55. I understand the SIO thereafter launched the EIP.

56. CISA did not launch the EIP, and the EIP is not a government organization.

57. CISA does not and has never funded the EIP.

58. Given its relationships with the election community, CISA connected the EIP with election stakeholders, such as NASS, NASED and CIS.

59. While I understand that the EIP engaged with entities such as CIS in relation to the 2020 election cycle, I do not know the nature of their relationship or the extent to which they worked together because that information was not shared with CISA. Further, I understand that the EIP flagged incidents for social media companies when content or behavior appeared to violate the company's terms of service, but CISA was not involved in the EIP's process. As discussed below, however, both CISA and the EIP received reports of potential election security-related disinformation from state and local election officials through CIS.

60. While the EIP briefed CISA regarding EIP's plans for the 2022 election cycle, the briefing was at a high-level and did not address if or how EIP may interact with CIS. I do not know how the EIP and CIS may have worked together in relation to the 2022 election cycle because CISA was not involved in or informed of any such work.

61. Certain Stanford University students have interned for CISA and also the SIO. Through their SIO work, I understand they may have supported the EIP. Any students who interned at CISA, however, should have performed only CISA work during their internship with the Agency. Similarly, they should not have performed any CISA work outside of their CISA internship, including while interning at SIO or supporting the EIP.

62. CISA has engaged with the EIP as it does with other nongovernmental organizations in the election community. For example, CISA, along with many others, has attended public briefings the EIP has provided.

63. Presently, CISA is not doing any work with the EIP.

VI. CISA's Disinformation-Related Work for the 2022 Election Cycle

64. In relation to the 2022 election cycle, CISA endeavored to mitigate the risks posed by disinformation targeting election infrastructure by sharing accurate information through CISA's Election Security Rumor vs. Reality webpage and amplifying the voices of state and local election officials through CISA's social media platforms and other public forums.

65. CISA supported the development of two EI-SCC and EIS-GCC Joint Managing Mis/Disinformation Working Group guides mentioned above: the Rumor Control Page Start-Up Guide and the MDM Planning and Incident Response Guide for Election Officials. *See supra* ¶ 40.

66. CISA released Tactics of Disinformation, a general disinformation resilience guide highlighting examples of the tactics use by foreign disinformation actors and outlining proactive

measures to mitigate the effectiveness of such tactics, *see supra* ¶ 14, and Halloween-themed messages on social media to build awareness to the risks posed by disinformation generally.

67. CISA partnered with the FBI to publish a PSA on information manipulation tactics related to the 2022 midterm elections. <https://www.cisa.gov/news-events/alerts/2022/10/07/fbi-and-cisa-publish-psa-information-manipulation-tactics-2022> (last visited April 24, 2023).

68. CISA participated in regular meetings often referred to as USG – Industry meetings. Participants typically included CISA, DHS, FBI, U.S. Department of Justice, the Office of the Director of National Intelligence, Google, Facebook, Twitter, Reddit, Microsoft, and Verizon Media. During such meetings, participants discussed general election security information such as election dates and high-level threat reporting. CISA often reported on election infrastructure security, key election timelines, and publications designed to promote resilience to disinformation, such as the Tactics of Disinformation. *See supra* ¶ 14, 66. CISA never flagged or reported potential disinformation for social media or technology companies during or in connection with the USG – Industry meetings.

69. CISA has not participated in the USG – Industry meetings since the 2022 general election.

VII. Historical Switchboarding Activity

70. One of the ways CISA supported the election community during the 2018 and 2020 election cycles was by transmitting potential election security-related disinformation identified by state and local election officials and other election stakeholders to social media platforms (referred to as “switchboarding”). Officials in Plaintiff States Missouri and Louisiana were among those whose transmitted election security-related disinformation to CISA or CIS for the purpose of it being shared with the social media companies. *See* Defs. Ex. 101 (MOLA_DEFSPROD_00007488; Defs. Ex. 102 (MOLA_DEFSPROD_00007647); Defs. Ex. 103

(MOLA_DEFSPROD_00010719); Defs. Ex. 104 (MOLA_DEFSPROD_00008681); Defs. Ex. 105 (MOLA_DEFSPROD_00010774 (NASS)); Defs. Ex. 106 (MOLA_DEFSPROD_00008610 (NASED)).

71. For the 2020 election cycle, much of the potential election security-related disinformation CISA received from state and local election officials was shared by election officials through CIS. In such instances, the election official would email the potential election security-related disinformation to CIS, who would forward the information to CISA and others, including the EIP.

72. CISA's protocol was to forward the potential election security-related disinformation to relevant social media or technology companies with the following notice stating that it was not requesting that the company take any particular action:

The Cybersecurity and Infrastructure Security Agency (CISA) of the U.S. Department of Homeland Security (DHS) is not the originator of this information. CISA is forwarding this information, unedited, from its originating source – this information has not been originated or generated by CISA. This information may also be shared with law enforcement or intelligence agencies.

CISA affirms that it neither has nor seeks the ability to remove or edit what information is made available on social media platforms. CISA makes no recommendations about how the information it is sharing should be handled or used by social media companies. Additionally, CISA will not take any action, favorable or unfavorable, toward social media companies based on decisions about how or whether to use this information.

In the event that CISA follows up to request further information, such a request is not a requirement or demand. Responding to this request is voluntary and CISA will not take any action, favorable or unfavorable, based on decisions about whether or not to respond to this follow-up request for information.

See, e.g., Defs. Ex. 107 (MOLA_DEFSPROD_00008499).

73. When CIS provided CISA with potential election security-related disinformation, CISA would copy CIS on the email to the social media or technology company for CIS's situational awareness.

74. I understand that during the 2020 election cycle CIS would share reports of potential election security-related disinformation with other organizations with which it had its own independent relationship. For example, I understand that CIS shared such information with the EIP for further analysis and with NASS and NASED for situational awareness. *See, e.g.*, MOLA_DEFSPROD_00008696 (attached hereto as Exhibit A).

75. At a certain point in the 2020 election cycle, CIS began forwarding the potential election security-related disinformation received from state and local election officials directly to the relevant social media or technology company and would include CISA on the email for situational awareness, as well as others, including the EIP. CISA took no action on these emails sent by CIS, other than frequently recording them in an internal CISA spreadsheet.

76. At some point in the 2020 election cycle, Twitter informed CISA that it was receiving the same potential election security-related disinformation from CISA, on behalf of SLTT election officials, as well as from CIS and the EIP. Twitter asked whether, to avoid duplication, only CISA could forward such information. In response to this, CISA discussed the duplicative reporting with CIS and the EIP in an attempt to minimize the duplication.

77. CISA did not fund CIS, the MS-ISAC or EI-ISAC for any of the work they provided in relation to the reporting of potential election security-related disinformation to social media or technology companies during the 2020 election cycle.

78. CISA did not engage in switchboarding for the 2022 election cycle and has no intention to engage in switchboarding for the next election.

79. While the CIS proposed that DHS fund CIS's work to identify and report inaccurate election information for the 2022 election cycle, DHS did not fund CIS, the MS-ISAC, or EI-ISAC for any reporting of potential election security-related disinformation to social media or technology companies they may have done during the 2022 election cycle.

80. As stated above, CISA has never provided funding to the EIP for any purpose, including the EIP's reporting of information for social media companies.

81. In addition, to the extent CIS, the MS-ISAC, or EI-ISAC, or the EIP reported potential election security-related disinformation to social media or technology companies in relation to the 2022 election cycle, CISA was not involved.

Pursuant to 28 U.S.C. § 1746, I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct to the best of my knowledge and belief.

Executed on this 28 day of April, 2023.

**GEOFFREY L
HALE**

Digitally signed by GEOFFREY L
HALE
Date: 2023.04.28 19:24:52 -04'00'

Geoffrey Hale
Lead, Election Security and Resilience
Cybersecurity and Infrastructure Security Agency

Exhibit A

From: Tracy Rohrbach [REDACTED]@fb.com]
Sent: 11/3/2020 7:07:19 PM
To: Misinformation Reports [misinformation@cisecurity.org]; Scully, Brian [REDACTED]@cisa.dhs.gov]; CISA Central [central@cisa.dhs.gov]; CFITF [cfitf@hq.dhs.gov]; tips@2020partnership.atlassian.net
Subject: Re: Case #CIS-MIS000142: Voter in MI alleges submitting 300 ballots

CAUTION: This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

Thank you for including me, I'm moving this through our processes now. I'll update you when I have more information.

Best,

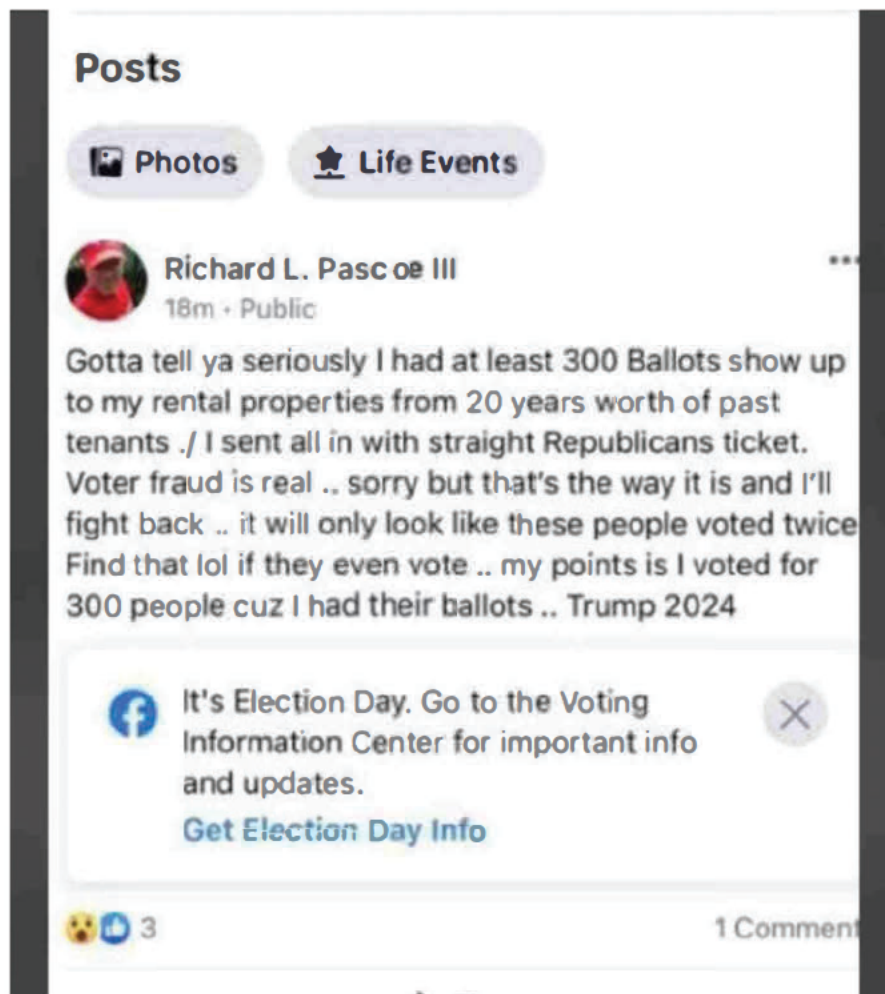
Tracy

From: Misinformation Reports <misinformation@cisecurity.org>
Sent: Tuesday, November 3, 2020 5:52 PM
To: Brian Scully [REDACTED]@cisa.dhs.gov]; Central CISA <central@cisa.dhs.gov>; cfif@hq.dhs.gov <cfif@hq.dhs.gov>; tips@2020partnership.atlassian.net <tips@2020partnership.atlassian.net>; Misinformation Reports <misinformation@cisecurity.org>
Cc: Tracy Rohrbach [REDACTED]@fb.com>
Subject: Case #CIS-MIS000142: Voter in MI alleges submitting 300 ballots

Brian and EIP, we have included Facebook in this report.

Misinformation report: citizen alleges on Facebook that he submitted 300 ballots

https://www.facebook.com/profile.php?id_1576601744



From: MS-ISACSOC

Sent: Tuesday, November 3, 2020 6:39 PM

To: Misinformation Reports <misinformation@cisecurity.org>

Cc: MS-ISACSOC <SOC@msisac.org>

Subject: FW: Michigan Voter Misinformation//Facebook

Please see below. Thanks.



Dylan Ginsburg

Security Operations Center Analyst II

Multi-State Information Sharing and Analysis Center (MS-ISAC)

Election Infrastructure Information Sharing and Analysis Center (EI-ISAC)

31 Tech Valley Drive

East Greenbush, NY 12061

24x7 Security Operations Center

SOC@cisecurity.org - 1-866-787-4722



From: Brown, Ashiya (MDOS) <[REDACTED]@michigan.gov>
Sent: Tuesday, November 3, 2020 6:35 PM
To: MS-ISAC SOC <SOC@msisac.org>
Subject: RE: Michigan Voter Misinformation//Facebook

Yes, please.

Ashiya Brown, MBA
Michigan Bureau of Elections
[REDACTED]@Michigan.gov
Office: [REDACTED]
Cell: [REDACTED]

From: MS-ISAC SOC <SOC@msisac.org>
Sent: Tuesday, November 3, 2020 6:32 PM
To: Brown, Ashiya (MDOS) <[REDACTED]@michigan.gov>; MS-ISAC SOC <SOC@msisac.org>
Subject: RE: Michigan Voter Misinformation//Facebook

CAUTION: This is an External email. Please send suspicious emails to abuse@michigan.gov

Ashiya,
Do we have your permission to share this with our federal partners by forwarding to our misinformation mailbox? Please see below.

Reports of Elections Infrastructure Misinformation ("Misinformation") submitted to the EI-ISAC via misinformation@cisecurity.org will be shared with the following organizations: (1) the applicable social media platform provider in order to address the Misinformation identified in the report; (2) the Cybersecurity & Infrastructure Security Agency and the Election Integrity Partnership, for analysis of the Misinformation, in conjunction with other relevant information, to identify potential threats to election security; (3) with the National Association for Secretaries of State and National Association of State Elections Directors for situational awareness. The Misinformation may also be shared with other federal agencies, as appropriate, for situational awareness or in the context of a law enforcement investigation.



Dylan Ginsburg

Security Operations Center Analyst II
Multi-State Information Sharing and Analysis Center (MS-ISAC)
Election Infrastructure Information Sharing and Analysis Center (EI-ISAC)
31 Tech Valley Drive
East Greenbush, NY 12061

24x7 Security Operations Center
SOC@cisecurity.org - 1-866-787-4722



MS-ISAC*
Multi-State Information
Sharing & Analysis Center*



**Elections
Infrastructure
ISAC**



From: Brown, Ashiya (MDOS) <[REDACTED]@michigan.gov>
Sent: Tuesday, November 3, 2020 6:27 PM
To: MS-ISAC SOC <SOC@msisac.org>
Subject: Michigan Voter Misinformation//Facebook

https://www.facebook.com/profile.php?id_1576601744

Hello,

The link below is a Michigan voter who is spreading misinformation being Facebook saying he voted for 300 people. We have had local law enforcement contact him and he has pulled the post. Hours later (about an hour ago) he started posting it again. Is this something you all can assist with getting Facebook to pull down? We have received a number of complaints about this post per hour.

https://www.facebook.com/profile.php?id_1576601744

Thank you!

Ashiya Brown, MBA
Michigan Bureau of Elections

Office: [REDACTED]

Cell: [REDACTED]

This message and attachments may contain confidential information. If it appears that this message was sent to you by mistake, any retention, dissemination, distribution or copying of this message and attachments is strictly prohibited. Please notify the sender immediately and permanently delete the message and any attachments.

This message and attachments may contain confidential information. If it appears that this message was sent to you by mistake, any retention, dissemination, distribution or copying of this message and attachments is strictly prohibited. Please notify the sender immediately and permanently delete the message and any attachments.

DEFENDANTS' EXHIBIT 98:

Last chance! Save up to 20% on CIS SecureSuite through April 2023 (<https://www.cisecurity.org/cis-securesuite>)

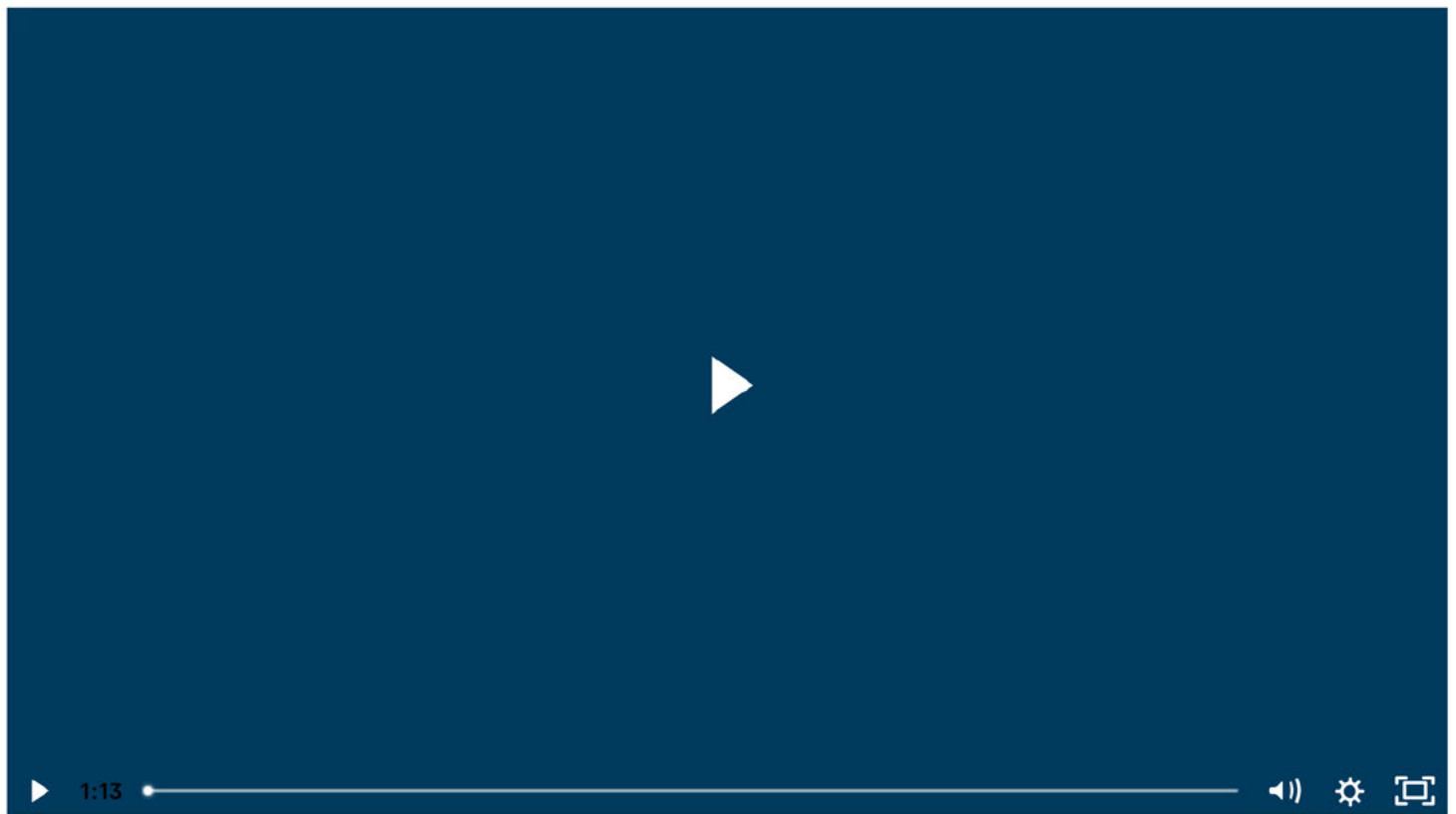


[Home](#) > [About us](#)

The Center for Internet Security, Inc. (CIS®) makes the connected world a safer place for people, businesses, and governments through our core competencies of collaboration and innovation.

We are a community-driven nonprofit, responsible for the CIS Controls® and CIS Benchmarks™, globally recognized best practices for securing IT systems and data. We lead a global community of IT professionals to continuously evolve these standards and provide products and services to proactively safeguard against emerging threats. Our CIS Hardened Images® provide secure, on-demand, scalable computing environments in the cloud.

CIS is home to the Multi-State Information Sharing and Analysis Center® (MS-ISAC®), the trusted resource for cyber threat prevention, protection, response, and recovery for U.S. State, Local, Tribal, and Territorial government entities, and the Elections Infrastructure Information Sharing and Analysis Center® (EI-ISAC®), which supports the rapidly changing cybersecurity needs of U.S. elections offices.



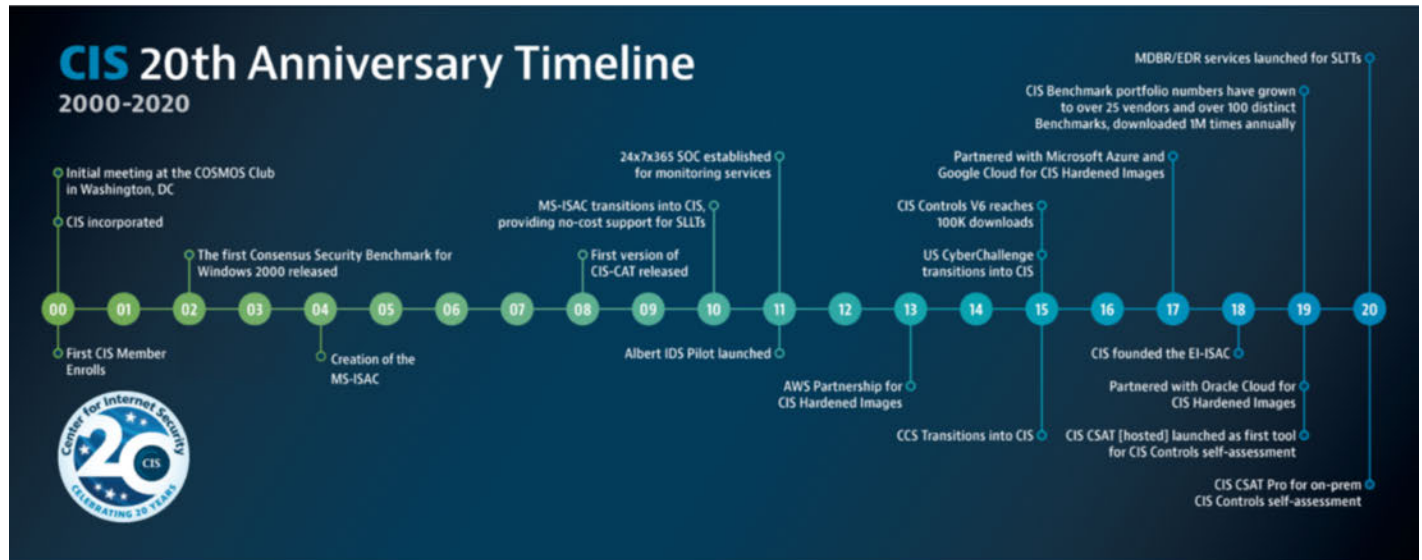
The CIS Vision:

Leading the global community to secure our ever-changing connected world.

The CIS Mission:

Our mission is to make the connected world a safer place by developing, validating, and promoting timely best practice solutions that help people, businesses, and governments protect themselves against pervasive cyber threats.

CIS Celebrates 20 Years:



Back in August of 2000, a small group of business and government leaders met at the legendary Cosmos Club in Washington, D.C. to discuss a concerning rash of cyber-attacks. From that meeting and others, a vision emerged for an independent, mission-driven, nonprofit organization dedicated to preventing and mitigating new cyber threats.

Today, CIS is the embodiment of that vision. Over the course of 20 years, we have been privileged to work with some of the best minds in the cybersecurity and IT professions. Through a global, collaborative effort, we have developed world-class standards in the form of the CIS Controls and CIS Benchmarks, along with specialized technology tools to help security practitioners implement and manage their cyber defenses.

Blog post: [CIS Celebrating 20 Years of Cybersecurity \(/insights/blog/cis-celebrating-20-years-of-cybersecurity\)](/insights/blog/cis-celebrating-20-years-of-cybersecurity)

Watch our anniversary video and read CIS Chief Evangelist, Tony Sager's special anniversary post. (/?p=21744&preview=true)



CIS LEADERSHIP PRINCIPLES

CIS CARES

IDEA ALLIANCE

ALAN PALLER LAUREATE PROGRAM

BOARD OF DIRECTORS

LEADERSHIP

CIS MEDIA PAGE

If you would like to inquire about having a CIS cybersecurity expert attend or speak at your event, please send your request to Events@cisecurity.org (<mailto:Events@cisecurity.org>)

[2022 Year in Review \(/insights/white-papers/2022-year-in-review\)](/insights/white-papers/2022-year-in-review)

WHITE PAPER 04.28.2023

[Living Off the Land: Scheduled Tasks \(/insights/white-papers/acceptable-use-policy-template-for-the-cis-controls\)](/insights/white-papers/acceptable-use-policy-template-for-the-cis-controls)

READ MORE

BLOG POST 04.27.2023

[Top 10 Malware Q1 2023 \(/insights/blog/top-10-malware-q1-2023\)](/insights/blog/top-10-malware-q1-2023)

READ MORE

WEBINAR 04.27.2023

[Effective Implementation of the CIS Benchmarks and CIS Controls \(/insights/webinar/effective-implementation-of-the-cis-benchmarks-and-cis-controls\)](/insights/webinar/effective-implementation-of-the-cis-benchmarks-and-cis-controls)

DEFENDANTS' EXHIBIT 99:

NewsRoom

3/1/23 Wash. Post (Wash., D.C.) A04
2023 WLNR 7536521

Washington Post, The (Washington, D.C.)
Copyright (c) 2023 The Washington Post

March 1, 2023

Issue DAILY
Section: Main (A Section)

What we know about covid-19 s origins, and what is still a mystery

Joel Achenbach

The precise origin of SARS-CoV-2, the coronavirus that causes covid-19, remains unknown and continues to be a source of contentious debate. Two theories dominate the conversation: a natural spillover from infected animals, and a "lab leak" associated with coronavirus research in Wuhan, China, the city where the first cases of an unusual pneumonia-like illness were reported.

President Biden in May 2021 asked intelligence agencies to probe the origins of the virus, but they were unable to reach a consensus. Most favored, with "low confidence," the natural spillover theory. Peer-reviewed scientific papers published last year bolstered the case that the virus came from animals sold at the Huanan Seafood Wholesale Market in Wuhan.

But critics of the natural spillover theory point out that investigators did not find any virus-infected animals that could have been the source of the outbreak. That fact was highlighted in a report issued last year by Republican staff on a Senate committee looking into the origin of the virus. The report also raised questions about safety protocols at a Wuhan laboratory. While not ruling out a natural spillover, the Republican staffers concluded that a "research-related incident" was the "most likely" origin.

Now House Republicans, newly in charge of their chamber, have opened a fresh probe of covid's origin.

What new evidence has emerged about the origin of covid-19?

There's not much that is new and compelling on the scientific front. But this is such an explosive issue that incremental developments can generate big headlines.

The newest political development is that the intelligence community produced an updated version of its 2021 report to Biden. By and large that assessment has not changed. But The Wall Street Journal reported on Feb. 26 that the updated assessment reveals the Energy Department has shifted from a neutral stance on the virus' origin to one favoring, with "low confidence," a lab leak.

The updated intelligence report remains classified, so it is unclear why the Energy Department changed its view.

Four other agencies and the National Intelligence Council continue to favor the natural origin with "low confidence." The FBI, however, continues to state with "moderate confidence" that it favors a laboratory origin.

Why is the Energy Department involved in covid investigations?

The Energy Department runs major national laboratories and spends billions every year on scientific research, including work on quantum physics and fusion energy. The covid origins analysis was performed by a little-known scientific team that specializes in emerging security threats, The Washington Post has reported.

National security adviser Jake Sullivan told CNN on Sunday that Biden asked for the national labs to be involved in the covid origin investigation "because he wants to put every tool at use to be able to figure out what happened here."

When asked about its new stance on a lab leak, a department spokesperson referred questions to the intelligence agencies, saying, "the Department of Energy continues to support the thorough, careful, and objective work of our intelligence professionals in investigating the origins of covid-19, as the President directed."

What evidence exists for a lab leak?

The Wuhan Institute of Virology is the primary focus of the lab leak conjectures, because it is a major research center that did extensive work on coronaviruses.

Many versions of the lab leak theory require some level of secrecy by researchers in China. But there are also scenarios that involve an accidental release of the virus without anyone realizing it. For example, researchers at the institute collect wild bats, which are ancestral sources of coronaviruses. Someone involved in this process could have inadvertently introduced the virus into the Wuhan population.

Proponents of a lab leak also point to experiments at the lab that manipulate viruses in ways that could make them more transmissible - "gain of function" experimentation. The goal of such research is to understand how a pathogen might evolve to become more of a threat, but critics have decried this as inviting disaster.

Supporters of the lab leak theory have pointed to an unfunded proposal for an experiment that, they argue, could be a recipe for making a virus like SARS-CoV-2. And one recent experiment at the Wuhan Institute of Virology, funded in part by the National Institutes of Health through a grant to the organization EcoHealth Alliance, has come under special scrutiny, creating a political headache for NIH officials.

That experiment could not have produced SARS-CoV-2, according to scientists who analyzed it. But critics believe this kind of viral manipulation - or some other type of experimentation that creates novel viruses or enhances their transmissibility - could have led to the creation of SARS-CoV-2.

That idea remains speculative. There is no evidence that the virus or its progenitor was in any laboratory before the outbreak in late 2019.

Chinese scientists have said they were not working with the virus. Chinese officials, however, have not been cooperative with international investigators, and have instead floated improbable theories, such as that the virus entered China in a shipment of frozen fish, or as the result of American biological research efforts.

The World Health Organization recently abandoned an effort to probe the origin of the virus, citing the political obstacles to the inquiry.

What is the evidence for a natural origin?

Many experts note that a natural origin would line up with the history of pandemics, which typically start with spillovers from animals - no laboratory help required. SARS, the previous coronavirus outbreak in China that began in 2002, emerged in a market spillover. It has been genetically traced back to horseshoe bats, and it infected humans via an intermediate species: civet cats sold in markets.

A large percentage of early SARS-CoV-2 infections documented in Wuhan were clustered around the Huanan Seafood Market, where animals were sold and butchered in conditions that scientists say were ripe for a spillover. Many species of animals sold there are now known to be capable of infection with SARS-CoV-2.

Two papers published last summer in the journal *Science* argued in favor of the market as the epicenter of the outbreak.

Based on genomic analysis of early infections, one paper argues there were at least two separate spillover events in the market, producing two distinct lineages of the virus. The other paper says the geographical clustering of early infections, combined with environmental samples showing traces of the virus in areas where animals were sold, point clearly to the market as the epicenter of the outbreak.

But the scientists favoring the market origin acknowledge that there are missing pieces in the narrative. They have not identified which animals were infected or where they came from. The market was closed and cleaned and the animals culled within a few days of the outbreak.

"Everything upstream of this - which animals, where did they come from, how it's all connected - is completely unknown at this stage," Kristian Andersen, an infectious-disease researcher at Scripps Research and co-author of both papers, said in a media briefing at the time.

Will we ever know the origin of covid?

The origin of covid has become so polarizing that it may never be resolved to widespread satisfaction. Because the issue is politicized, it is vulnerable to motivated reasoning - interpreting facts to fit a preferred narrative.

The narrative could change dramatically with a new scientific or investigatory revelation that produces unassailable and unambiguous evidence. For example, a whistleblower in a laboratory could reveal credible evidence of the presence of SARS-CoV-2 in a research facility before the outbreak. Or, researchers could find the progenitor of SARS-CoV-2 in archived tissue samples taken from commercially trafficked animals.

In the meantime, the contentious situation has put increased attention on whether laboratory research on viruses is worth the risk of an accident.

There is a significant, ongoing divide among scientists about the safety of laboratory research that involves the manipulation of pathogens. Lab leaks can happen. Research on viruses may involve manipulating them in ways that could, in theory, lead to an accident - and a pandemic.

Due to ongoing concerns about research safety, the National Science Advisory Board for Biosecurity has issued a preliminary report calling for tightening of oversight of research on potential pathogens. Those changes have been in process for many years and are not a response to the lab leak theory. But questions about covid's origin inevitably shadow any discussion about how to balance the risks and benefits of pathogen research.

On Feb. 26, Gerald Parker, a Texas A&M University professor and chair of the biosafety board, wrote on Twitter, "We have a moral obligation to determine to the best of our ability how SARS2 emerged to cause the worst pandemic in over 100 years."

---- Index References ----

Company: TEXAS A&M UNIVERSITY; Federal Bureau of Investigation; National Institutes of Health; ECOHEALTH ALLIANCE INC.; Scripps Research Digital Trials Center; Wuhan Institute of Virology, CAS; World Health Organization Medical Research Council

News Subject: (Emerging Market Countries (1EM65); United Nations (1UN54); World Health Organization (1WO40); World Organizations (1IN77))

Industry: (Coronavirus (1CV19); Healthcare (1HE06); Infectious Diseases (1IN99); SARS (1SA26); Upper Respiratory Disease (1UP05); Viral (1VI15))

Region: (Asia (1AS61); China (1CH15); Eastern Asia (1EA61); Far East (1FA27))

Language: EN

Other Indexing: (Senate; Energy Department; National Intelligence Council; CNN; Department of Energy; National Science Advisory Board for Biosecurity; Texas A&M University; FBI; National Institutes of Health; EcoHealth Alliance; Scripps Research; Wuhan Institute of Virology; World Health Organization)

Edition: SU

Word Count: 1442

End of Document

© 2023 Thomson Reuters. No claim to original U.S. Government Works.

NewsRoom

DEFENDANTS' EXHIBIT 100:

Sent: 9/15/2020 9:12:17 AM
To: Sandra Luff [sandyluff@fb.com]; Saleela Salahuddin [saleelas@fb.com]
Subject: FW: Fwd:
Attachments: Screensho.jpg; Screensho.jpg; Screensho.jpg; Screensho.jpg; Screensho.jpg

Good morning Sandy and Saleela,

Please see attached reporting from LA Secretary of State's Office. They believe this is a coordinated disinfo campaign and asked us to pass along. I am going to see if I can get any info on the originator of the message. There's a second email I will also be forwarding.

Thanks,
Brian

Neither the U.S. Department of Homeland Security (DHS) nor the Department's Countering Foreign Interference (CFI) Task Force is the originator of this information. The CFI Task Force is forwarding this information, unedited, from its originating source – this information has not been originated or generated by DHS or the CFI Task Force. This information may also be shared with law enforcement or intelligence agencies.

DHS affirms that it neither has nor seeks the ability to remove or edit what information is made available on social media platforms. DHS makes no recommendations about how the information it is sharing should be handled or used by social media companies. Additionally, DHS will not take any action, favorable or unfavorable, toward social media companies based on decisions about how or whether to use this information.

In the event that the CFI Task Force follows up to request further information, such a request is not a requirement or demand. Responding to this request is voluntary and DHS will not take any action, favorable or unfavorable, based on decisions about whether or not to respond to this follow-up request for information.

From: Masterson, Matthew <Matthew.Masterson@cisa.dhs.gov>
Sent: Monday, September 14, 2020 10:30 PM
To: Scully, Brian <brian.scully1@cisa.dhs.gov>
Cc: Hale, Geoffrey <Geoffrey.Hale@cisa.dhs.gov>; Snell, Allison <Allison.Snell@cisa.dhs.gov>; Dragseth, John <John.Dragseth@cisa.dhs.gov>
Subject: Fwd: Fwd:

Scully,

See attached from LA SOS. He called and views this as a coordinated disinfo campaign. Please pass ASAP to Facebook and FBI as well as other platforms.

Matthew V. Masterson
Senior Cybersecurity Advisor
Department of Homeland Security
Cybersecurity & Infrastructure Security Agency (CISA)
(202)309-1585

Matthew.Masterson@cisa.dhs.gov

From: Sherri Hadskey <sherri.hadskey@sos.la.gov>

Sent: Monday, September 14, 2020 10:27:22 PM

To: Masterson, Matthew <Matthew.Masterson@cisa.dhs.gov>; McKee, Jeffery <Jeffery.McKee@cisa.dhs.gov>

Subject: Fwd:

CAUTION: This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

Here are some of the messages.

Thank you,

Sherri Wharton Hadskey, CERA

Commissioner of Elections

Elections Division

Secretary of State Kyle Ardoin

225-922-2486 (o)

225-922-2910 (f)

225-603-8583 (c)

www.sos.la.gov

----- Forwarded message -----

From: <2259166486@mms.att.net>

Date: Mon, Sep 14, 2020 at 9:16 PM

Subject:

To: <sherri.hadskey@sos.la.gov>

DEFENDANTS' EXHIBIT 101:

From: Scully, Brian [/O=EXCHANGELABS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=7CA10604AEE04B1DAB53DC9F884130BD-SCULLY, BRI]
Sent: 9/15/2020 9:18:33 AM
To: Stacia Cardille [scardille@twitter.com]; Lisa Roman [lroman@twitter.com]
Subject: FW: Fwd:
Attachments: Screensho.jpg; Screensho.jpg; Screensho.jpg; Screensho.jpg; Screensho.jpg

Good morning Stacia and Lisa,

We received the attached from the LA Secretary of State's office. They view these as a coordinated disinfo campaign. It's from Facebook, but I thought it might be something you all would see on Twitter, so sent along. I'm trying to get more info on where the posts originated and will send any additional info I receive. There's a second email I'll also send.

Thanks,
Brian

Neither the U.S. Department of Homeland Security (DHS) nor the Department's Countering Foreign Interference (CFI) Task Force is the originator of this information. The CFI Task Force is forwarding this information, unedited, from its originating source – this information has not been originated or generated by DHS or the CFI Task Force. This information may also be shared with law enforcement or intelligence agencies.

DHS affirms that it neither has nor seeks the ability to remove or edit what information is made available on social media platforms. DHS makes no recommendations about how the information it is sharing should be handled or used by social media companies. Additionally, DHS will not take any action, favorable or unfavorable, toward social media companies based on decisions about how or whether to use this information.

In the event that the CFI Task Force follows up to request further information, such a request is not a requirement or demand. Responding to this request is voluntary and DHS will not take any action, favorable or unfavorable, based on decisions about whether or not to respond to this follow-up request for information.

From: Masterson, Matthew <Matthew.Masterson@cisa.dhs.gov>
Sent: Monday, September 14, 2020 10:30 PM
To: Scully, Brian <brian.scully1@cisa.dhs.gov>
Cc: Hale, Geoffrey <Geoffrey.Hale@cisa.dhs.gov>; Snell, Allison <Allison.Snell@cisa.dhs.gov>; Dragseth, John <John.Dragseth@cisa.dhs.gov>
Subject: Fwd: Fwd:

Scully,

See attached from LA SOS. He called and views this as a coordinated disinfo campaign. Please pass ASAP to Facebook and FBI as well as other platforms.

Matthew V. Masterson
Senior Cybersecurity Advisor
Department of Homeland Security

Cybersecurity & Infrastructure Security Agency (CISA)

(202)309-1585

Matthew.Masterson@cisa.dhs.gov

From: Sherri Hadskey <sherri.hadskey@sos.la.gov>

Sent: Monday, September 14, 2020 10:27:22 PM

To: Masterson, Matthew <Matthew.Masterson@cisa.dhs.gov>; McKee, Jeffery <Jeffery.McKee@cisa.dhs.gov>

Subject: Fwd:

CAUTION: This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

Here are some of the messages.

Thank you,

Sherri Wharton Hadskey, CERA

Commissioner of Elections

Elections Division

Secretary of State Kyle Ardoin

225-922-2486 (o)

225-922-2910 (f)

225-603-8583 (c)

www.sos.la.gov

----- Forwarded message -----

From: <2259166486@mms.att.net>

Date: Mon, Sep 14, 2020 at 9:16 PM

Subject:

To: <sherri.hadskey@sos.la.gov>

DEFENDANTS' EXHIBIT 102:

From: Scully, Brian [/O=EXCHANGELABS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=7CA10604AEE04B1DAB53DC9F884130BD-SCULLY, BRI]
Sent: 9/15/2020 9:19:16 AM
To: Stacia Cardille [scardille@twitter.com]; Lisa Roman [lroman@twitter.com]
Subject: FW: Coord Disinfo
Attachments: Screensho.jpg

Here's the second email.

Thanks,
Brian

Neither the U.S. Department of Homeland Security (DHS) nor the Department's Countering Foreign Interference (CFI) Task Force is the originator of this information. The CFI Task Force is forwarding this information, unedited, from its originating source – this information has not been originated or generated by DHS or the CFI Task Force. This information may also be shared with law enforcement or intelligence agencies.

DHS affirms that it neither has nor seeks the ability to remove or edit what information is made available on social media platforms. DHS makes no recommendations about how the information it is sharing should be handled or used by social media companies. Additionally, DHS will not take any action, favorable or unfavorable, toward social media companies based on decisions about how or whether to use this information.

In the event that the CFI Task Force follows up to request further information, such a request is not a requirement or demand. Responding to this request is voluntary and DHS will not take any action, favorable or unfavorable, based on decisions about whether or not to respond to this follow-up request for information.

From: Masterson, Matthew <Matthew.Masterson@cisa.dhs.gov>
Sent: Monday, September 14, 2020 10:30 PM
To: Scully, Brian <brian.scully1@cisa.dhs.gov>
Cc: Hale, Geoffrey <Geoffrey.Hale@cisa.dhs.gov>; Snell, Allison <Allison.Snell@cisa.dhs.gov>; Dragseth, John <John.Dragseth@cisa.dhs.gov>
Subject: Fwd: Fwd:

Email 2 of 2.

Matthew V. Masterson
Senior Cybersecurity Advisor
Department of Homeland Security
Cybersecurity & Infrastructure Security Agency (CISA)
(202)309-1585
Matthew.Masterson@cisa.dhs.gov

From: Sherri Hadskey <sherri.hadskey@sos.la.gov>
Sent: Monday, September 14, 2020 10:28 PM

To: Masterson, Matthew; McKee, Jeffery

Subject: Fwd:

CAUTION: This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

Thank you,

Sherri Wharton Hadskey, CERA

Commissioner of Elections

Elections Division

Secretary of State Kyle Ardoin

225-922-2486 (o)

225-922-2910 (f)

225-603-8583 (c)

www.sos.la.gov

----- Forwarded message -----

From: <2259166486@mms.att.net>

Date: Mon, Sep 14, 2020 at 9:16 PM

Subject:

To: <sherri.hadskey@sos.la.gov>

DEFENDANTS' EXHIBIT 103:

From: Rachel Holland [rachelholland@fb.com]
Sent: 11/5/2020 1:25:18 PM
To: Misinformation Reports [misinformation@cisecurity.org]; Scully, Brian [brian.scully1@cisa.dhs.gov]; CISA Central [central@cisa.dhs.gov]; CFITF [cfitf@hq.dhs.gov]; tips@2020partnership.atlassian.net
Subject: Re: Case #CIS-MIS000171: Facebook post regarding counting early ballots in Greene County, KY

CAUTION: This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

I can confirm that this has been closed out and Greene County, MO has been informed. Thanks, RH

From: Misinformation Reports <misinformation@cisecurity.org>
Date: Thursday, November 5, 2020 at 8:32 AM
To: Brian Scully <brian.scully1@cisa.dhs.gov>, Central CISA <central@cisa.dhs.gov>, "cfitf@hq.dhs.gov" <cfitf@hq.dhs.gov>, "tips@2020partnership.atlassian.net" <tips@2020partnership.atlassian.net>, Misinformation Reports <misinformation@cisecurity.org>
Cc: Rachel Holland <rachelholland@fb.com>
Subject: Case #CIS-MIS000171: Facebook post regarding counting early ballots in Greene County, KY

Brian and EIP, we included Facebook in this report.

Misinformation report: Facebook post regarding counting early ballots in Greene County, KY

From: Mark Peck <MPeck@greenecountymo.gov>
Sent: Thursday, November 5, 2020 9:03 AM
To: Misinformation Reports <misinformation@cisecurity.org>
Subject: Misinformation FB comment

Hello,

I'd like to report a misinformation post in the comment section of a Facebook post on our local news outlet, KY3. The post

url: <https://www.facebook.com/ky3news>

post title: Greene County election officials begin counting early ballots

date/time posted: 11/3/2020 11:51am

It appears the news outlet deleted the comment after our County Clerk's office made them aware of the misinformation. I have attached a copy of the FB post, and a screenshot of the comment. The false comment was made by "Calypso Nylund" who has never worked for the County Clerk's office. The Clerk's office issued a press release in regards to this comment.

As far as official contact info goes, I'm not sure whose you need, so I'll give you multiple.

My contact info is: Mark Peck, mpeck@greenecountymo.gov, 417-868-4145

County clerk: Shane Schoeller, sschoeller@greenecountymo.gov, 417-868-6359

News outlet: I don't have this yet, but if you need it I can get it.

Please let me know if there is anything else I can send you.

Thank you,

Mark Peck
Sr. Information Security Engineer
Greene County Information Systems
(417) 868-4145

.....

This message and attachments may contain confidential information. If it appears that this message was sent to you by mistake, any retention, dissemination, distribution or copying of this message and attachments is strictly prohibited. Please notify the sender immediately and permanently delete the message and any attachments.

.....

DEFENDANTS' EXHIBIT 104:

From: Scully, Brian [/O=EXCHANGELABS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=7CA10604AEE04B1DAB53DC9F884130BD-SCULLY, BRI]
Sent: 6/12/2020 9:55:05 AM
To: Lisa Roman [lroman@twitter.com]
CC: Stacia Cardille [scardille@twitter.com]
Subject: RE: FW: NASS/NASED Twitter Spam from Korea

They've sent me all their case numbers. Let me know if you need those.

Brian

From: Lisa Roman <lroman@twitter.com>
Sent: Friday, June 12, 2020 9:28 AM
To: Scully, Brian <brian.scully1@cisa.dhs.gov>
Cc: Stacia Cardille <scardille@twitter.com>
Subject: Re: FW: NASS/NASED Twitter Spam from Korea

CAUTION: This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

:)

On Fri, Jun 12, 2020 at 9:27 AM Scully, Brian <brian.scully1@cisa.dhs.gov> wrote:

LOL...they can be a bit aggressive. Apologies for the extra emails.

Brian

From: Lisa Roman <lroman@twitter.com>
Sent: Friday, June 12, 2020 9:25 AM
To: Scully, Brian <brian.scully1@cisa.dhs.gov>
Cc: Stacia Cardille <scardille@twitter.com>
Subject: Re: FW: NASS/NASED Twitter Spam from Korea

CAUTION: This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

Hi Brian,

Thanks for your email. We received this same info from Maria yesterday and again this morning. Sometimes we will need more than 24 hours to get to the bottom of something and be able to provide feedback.

Thanks!

Lisa

On Fri, Jun 12, 2020 at 9:22 AM Scully, Brian <brian.scully1@cisa.dhs.gov> wrote:

FYI – Please see below reporting from NASS. I’m also going to send a list of accounts in a separate email. I’ve asked NASS and NASED to provide me some information on how they reported to Twitter.

Regards,

Brian

Neither the Cybersecurity and Infrastructure Security Agency (CISA) nor CISA’s Countering Foreign Interference (CFI) Task Force is the originator of this information. The CFI Task Force is forwarding this information, unedited, from its originating source – this information has not been originated or generated by CISA or the CFI Task Force. This information may also be shared with law enforcement or intelligence agencies. CISA affirms that it neither has nor seeks the ability to remove or edit what information is made available on social media platforms. CISA makes no recommendations about how the information it is sharing should be handled or used by social media companies. Additionally, CISA will not take any action, favorable or unfavorable, toward social media companies based on decisions about how or whether to use this information.

In the event that the CFI Task Force follows up to request further information, such a request is not a requirement or demand. Responding to this request is voluntary and CISA will not take any action, favorable or unfavorable, based on decisions about whether or not to respond to this follow-up request for information.

From: Maria Benson <mbenson@sso.org>

Sent: Friday, June 12, 2020 9:13 AM

To: Scully, Brian <brian.scully1@cisa.dhs.gov>

Cc: Amy Cohen <acohen@nased.org>; Reynolds, Leslie <reynolds@sso.org>

Subject: RE: NASS/NASED Twitter Spam from Korea

CAUTION: This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

I wanted to screen shot one of the notifications to give you an idea (below and attached)



MaskpackmanTV 🇺🇸 @MaskpackmanT · 24m

Replying to @MaskpackmanT @USEmbassySeoul and 2 others

🇰🇷 ❤️ Korean Man 🇰🇷 @pUGP5yu2v5uPoqV · 14h

외국 신문에 실린 대한민국 개망신
짜장면 배달보다 못한 유권자표 관리
국민 주권은 혈스장에 처박히고, 플라스틱 박스에 담기고 현금노예로 팔리
는 참담한 나라, 사상교육에 매수된 니들 청년 눈에는 안보이는가 ♡썩은 지
성이 더 대한민국 의 미래를 더 암담 하게 한다♡
곳간은 비다 깨졌도다



Maria Benson

Director of Communications

National Association of Secretaries of State (NASS)

444 N. Capitol Street NW, Suite 401 | Washington, DC 20001

Desk: 202-624-3528 | Cell: 423-504-1351

www.nass.org



From: Maria Benson

Sent: Friday, June 12, 2020 9:05 AM

To: 'Scully, Brian' <brian.scully1@cisa.dhs.gov>

Cc: Amy Cohen <acohen@nased.org>; 'Reynolds' <reynolds@sso.org>

Subject: NASS/NASED Twitter Spam from Korea

Importance: High

Hi Brian,

I'm not sure if this is something you can help with or not, but at the very least I wanted to give you a heads up. For the last 2 days, both Amy and I reported numerous potential fake accounts that were spamming @NASSorg, @USEmbassySeoul and @NASEDorg on South Korean election issues. Many were just set up in the last month or so with black umbrellas as their profile picture and they're saying the Korean election was rigged, hacked, etc. Most of the tweets are in Korean so I can't obviously read them, but the sheer volume is concerning...it's becoming a machine almost. Amy and I both have hundreds of notifications to our accounts.

For context, we recently held an event with our members, South Korea and the U.S. State Department. Amy and I both submitted multiple cases through the partner support portal and contacted Stacia and Lisa. We've asked for updates, but haven't heard anything.

Any advice or thoughts?

Thanks as always,

Maria Benson

Director of Communications

National Association of Secretaries of State (NASS)

444 N. Capitol Street NW, Suite 401 | Washington, DC 20001

Desk: 202-624-3528 | Cell: 423-504-1351

www.nass.org



Disclaimer

The information contained in this communication from the sender is confidential. It is intended solely for use by the recipient and others authorized to receive it. If you are not the recipient, you are hereby notified that any disclosure, copying, distribution or taking action in relation of the contents of this information is strictly prohibited and may be unlawful.

This email has been scanned for viruses and malware, and may have been automatically archived by **Mimecast Ltd**, an innovator in Software as a Service (SaaS) for business. Providing a **safer** and **more useful** place for your human generated data. Specializing in; Security, archiving and compliance. To find out more [Click Here](#).

DEFENDANTS' EXHIBIT 105:

From: Todd O'Boyle [toboyle@twitter.com]
Sent: 11/23/2020 5:10:38 PM
To: Scully, Brian [brian.scully1@cisa.dhs.gov]
CC: CFITF [cfittf@hq.dhs.gov]; Stacia Cardille [scardille@twitter.com]; Todd O'Boyle [toddoboyale@twitter.com]
Subject: Re: FW: CIS-MIS000220 - allegations that Georgia is purging voters

CAUTION: This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

Hi Brian - this Tweet was not determined to be a violation of our rule

On Mon, Nov 23, 2020 at 11:32 AM Todd O'Boyle <toboyle@twitter.com> wrote:
Thanks Brian - we will escalate.

On Mon, Nov 23, 2020 at 11:31 AM Scully, Brian <brian.scully1@cisa.dhs.gov> wrote:
Stacia and Todd,

Please see the below report from NASED.

Thanks,
Brian

The Cybersecurity and Infrastructure Security Agency (CISA) of the U.S. Department of Homeland Security (DHS) is not the originator of this information. CISA is forwarding this information, unedited, from its originating source – this information has not been originated or generated by CISA. This information may also be shared with law enforcement or intelligence agencies.

CISA affirms that it neither has nor seeks the ability to remove or edit what information is made available on social media platforms. CISA makes no recommendations about how the information it is sharing should be handled or used by social media companies. Additionally, CISA will not take any action, favorable or unfavorable, toward social media companies based on decisions about how or whether to use this information.

In the event that CISA follows up to request further information, such a request is not a requirement or demand. Responding to this request is voluntary and CISA will not take any action, favorable or unfavorable, based on decisions about whether or not to respond to this follow-up request for information.

From: Misinformation Reports <misinformation@cisecurity.org>
Sent: Monday, November 23, 2020 10:55 AM
To: Scully, Brian <brian.scully1@cisa.dhs.gov>; CISA Central <central@cisa.dhs.gov>; CFITF <cfittf@hq.dhs.gov>; tips@2020partnership.atlassian.net; Misinformation Reports <misinformation@cisecurity.org>
Subject: CIS-MIS000220 - allegations that Georgia is purging voters

CAUTION: This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

Misinformation Report: Tweet alleging Georgia is purging voters

From: Amy Cohen <acohen@nased.org>
Sent: Monday, November 23, 2020 10:01 AM
To: Misinformation Reports <misinformation@cisecurity.org>
Subject: Tweet

<https://twitter.com/pattyarquette/status/1330730873445117954?s=21>

Georgia is not purging voters. We're within 90 days of the election, so that would be a violation of federal law.

Amy Cohen
Executive Director
National Association of State Election Directors (NASED)

.....

This message and attachments may contain confidential information. If it appears that this message was sent to you by mistake, any retention, dissemination, distribution or copying of this message and attachments is strictly prohibited. Please notify the sender immediately and permanently delete the message and any attachments.

.....

DEFENDANTS' EXHIBIT 106:

From: Scully, Brian [/O=EXCHANGELABS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=7CA10604AEE04B1DAB53DC9F884130BD-SCULLY, BRI]
Sent: 10/28/2020 6:29:07 PM
To: Stacia Cardille [scardille@twitter.com]; Todd O'Boyle [toddoboyle@twitter.com]; Neema Guliani [nguliani@twitter.com]
CC: CFITF [cfitf@hq.dhs.gov]; misinformation@cisecurity.org
Subject: FW: Case #CIS-MIS000087: misinformation tweets regarding mail-in ballots
Attachments: Gabe_kTweet.png; ReeseRe48384159Tweet.png

Please see below report from Washington.

Regards,
Brian

The Cybersecurity and Infrastructure Security Agency (CISA) of the U.S. Department of Homeland Security (DHS) is not the originator of this information. CISA is forwarding this information, unedited, from its originating source – this information has not been originated or generated by CISA. This information may also be shared with law enforcement or intelligence agencies.

CISA affirms that it neither has nor seeks the ability to remove or edit what information is made available on social media platforms. CISA makes no recommendations about how the information it is sharing should be handled or used by social media companies. Additionally, CISA will not take any action, favorable or unfavorable, toward social media companies based on decisions about how or whether to use this information.

In the event that CISA follows up to request further information, such a request is not a requirement or demand. Responding to this request is voluntary and CISA will not take any action, favorable or unfavorable, based on decisions about whether or not to respond to this follow-up request for information.

From: Misinformation Reports <misinformation@cisecurity.org>
Sent: Wednesday, October 28, 2020 6:14 PM
To: Scully, Brian <brian.scully1@cisa.dhs.gov>; CISA Central <central@cisa.dhs.gov>; CFITF <cfitf@hq.dhs.gov>; tips@2020partnership.atlassian.net; Misinformation Reports <misinformation@cisecurity.org>
Subject: Case #CIS-MIS000087: misinformation tweets regarding mail-in ballots

CAUTION: This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

Two misinformation tweets regarding mail-in ballots in Washington state.

From: Jacob, Nick <nick.jacob@sos.wa.gov>
Sent: Wednesday, October 28, 2020 5:56 PM
To: Misinformation Reports <misinformation@cisecurity.org>
Cc: Lori Augino <lori.augino@sos.wa.gov>; Zabel, Kylee <kylee.zabel@sos.wa.gov>; Boyal, Kiran <kiran.boyal@sos.wa.gov>
Subject: Possible misinformation on Twitter

Hello,

I wanted to flag two tweets with possible misinformation about the election here in Washington state.

https://twitter.com/gabe_k/status/1321523966683406336 -- Ballots that are postmarked by Election Day are accepted up to 20 days after Election Day. This tweet is false.

<https://twitter.com/ReeseRe48384159/status/1321563373020983297> -- Please see the information cited above. This tweet is also false.

My name is Nick Jacob, and I'm an Executive Receptionist for the Washington Office of the Secretary of State. I can be reached via this email or the number listed in my signature block below. My cell phone is monitored after hours if I need to be reached urgently.

I am also copying Washington State Elections Director Lori Augino, Office of the Secretary of State Communications Director Kylee Zabel, and our Web and Social Media Coordinator Kiran Boyal.

Please let me know if you have any questions or need additional information.

Thank you.

-Nick

Nick Jacob

Office of the Secretary of State

Cell: (425) 772-7204



.....

This message and attachments may contain confidential information. If it appears that this message was sent to you by mistake, any retention, dissemination, distribution or copying of this message and attachments is strictly prohibited. Please notify the sender immediately and permanently delete the message and any attachments.

.....

DEFENDANTS' EXHIBIT 107:

From: Stacia Cardille [scardille@twitter.com]
Sent: 11/11/2020 12:11:52 AM
To: Scully, Brian [brian.scully1@cisa.dhs.gov]
CC: Todd O'Boyle [toddoboyles@twitter.com]; Neema Guliani [nguliani@twitter.com]; Twitter Government & Politics [gov@twitter.com]; CFITF [cfitf@hq.dhs.gov]; Misinformation Reports [misinformation@cisecurity.org]
Subject: Re: FW: Case #CIS-MIS000195: allegations of election fraud with Dominion voting equipment in WA state

CAUTION: This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

Thank you. All Tweets have been labeled, with the exception of two from @SeattleSuze. Those two Tweets were not found to violate our policies.

Thank you,
Stacia

On Tue, Nov 10, 2020 at 7:25 PM Stacia Cardille <scardille@twitter.com> wrote:
Thanks, Brian. We will escalate.

On Tue, Nov 10, 2020 at 7:23 PM Scully, Brian <brian.scully1@cisa.dhs.gov> wrote:
Good evening Twitter,

Please see the below report from Washington.

Thanks,
Brian

The Cybersecurity and Infrastructure Security Agency (CISA) of the U.S. Department of Homeland Security (DHS) is not the originator of this information. CISA is forwarding this information, unedited, from its originating source – this information has not been originated or generated by CISA. This information may also be shared with law enforcement or intelligence agencies.

CISA affirms that it neither has nor seeks the ability to remove or edit what information is made available on social media platforms. CISA makes no recommendations about how the information it is sharing should be handled or used by social media companies. Additionally, CISA will not take any action, favorable or unfavorable, toward social media companies based on decisions about how or whether to use this information.

In the event that CISA follows up to request further information, such a request is not a requirement or demand. Responding to this request is voluntary and CISA will not take any action, favorable or unfavorable, based on decisions about whether or not to respond to this follow-up request for information.

From: Misinformation Reports <misinformation@cisecurity.org>
Sent: Tuesday, November 10, 2020 7:17 PM

To: Scully, Brian <brian.scully1@cisa.dhs.gov>; CISA Central <central@cisa.dhs.gov>; CFITF <cfittf@hq.dhs.gov>; tips@2020partnership.atlassian.net; Misinformation Reports <misinformation@cisecurity.org>

Subject: Case #CIS-MIS000195: allegations of election fraud with Dominion voting equipment in WA state

CAUTION: This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

Misinformation report: twelve (12) tweets alleging election fraud with Dominion voting equipment in Washington state.

From: Jacob, Nick <nick.jacob@sos.wa.gov>

Sent: Tuesday, November 10, 2020 7:03 PM

To: Misinformation Reports <misinformation@cisecurity.org>

Cc: Lori Augino <lori.augino@sos.wa.gov>; Zabel, Kylee <kylee.zabel@sos.wa.gov>; Boyal, Kiran <kiran.boyal@sos.wa.gov>

Subject: Misinformation on Twitter

Hello,

I wanted to flag the following tweets that include misinformation and/or false allegations of election fraud. There is no evidence to back any of these claims. There have been no reports or indications of fraudulent activity in Washington state for the 2020 general election.

Franklin County is the only county in Washington state that uses a version of Dominion software and hardware. The system in use has been certified, and we are not aware of any issues.

No counties in Washington state use GEMS.

Additionally, each county conducts post-election audits in the days after the election that are publicly observable, which provides another layer of protection to ensure the results they certify later this month are accurate. At the end of the certification period, each county will publish a reconciliation report that discloses details about all of the ballots issued, received, counted, and rejected during this election.

<https://twitter.com/LuvMyCountry7/status/1326303394147921920>

<https://twitter.com/seattleSuze/status/1326208987348398080>

<https://twitter.com/seattleSuze/status/1326209828717436928>

<https://twitter.com/MatthewMacphe17/status/1326212450585210880>

<https://twitter.com/MatthewMacphe17/status/1326211588089470976>

<https://twitter.com/MatthewMacphe17/status/1326204530543882240>

<https://twitter.com/MatthewMacphe17/status/1326202866567049216>

<https://twitter.com/Katrina64718085/status/1326311025738575872>

<https://twitter.com/Maga2020Rules/status/1326187323566948352>

<https://twitter.com/lazalere/status/1326082445196681216>

<https://twitter.com/TerenaHimpel/status/1326006222034665472>

<https://twitter.com/LolaTwelve/status/1325934941503250433>

My name is Nick Jacob, and I'm an Executive Receptionist for the Washington Office of the Secretary of State. I can be reached via this email or the number listed in my signature block below. My cell phone is monitored after hours if I need to be reached urgently.

I am also copying Washington State Elections Director Lori Augino, Office of the Secretary of State Communications Director Kylee Zabel, and our Web and Social Media Coordinator Kiran Boyal.

Please let me know if you have any questions or need additional information.

Thank you.

-Nick

Nick Jacob

Office of the Secretary of State

Cell: (425) 772-7204

 **Secretary of State**
Tim Augino



.....

This message and attachments may contain confidential information. If it appears that this message was sent to you by mistake, any retention, dissemination, distribution or copying of this message and attachments is strictly prohibited. Please notify the sender immediately and permanently delete the message and any attachments.

.....

DEFENDANTS' EXHIBIT 108:

From: Todd O'Boyle [toboyle@twitter.com]
Sent: 10/27/2020 4:38:48 PM
To: Scully, Brian [brian.scully1@cisa.dhs.gov]
CC: Stacia Cardille [scardille@twitter.com]; Todd O'Boyle [toddoboyale@twitter.com]; Neema Guliani [nguliani@twitter.com]; CFITF [cfitf@hq.dhs.gov]; Misinformation Reports [misinformation@cisecurity.org]
Subject: Re: FW: Case #CIS-MIS000075: Misinformation tweet regarding re-voting

CAUTION: This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

Update Brian:

Our team concluded that the Tweet was not in violation of our Civic Integrity Policy.

Best.

TO

On Tue, Oct 27, 2020 at 4:09 PM Scully, Brian <brian.scully1@cisa.dhs.gov> wrote:

Please see below report from Washington.

Thanks,

Brian

The Cybersecurity and Infrastructure Security Agency (CISA) of the U.S. Department of Homeland Security (DHS) is not the originator of this information. CISA is forwarding this information, unedited, from its originating source – this information has not been originated or generated by CISA. This information may also be shared with law enforcement or intelligence agencies.

CISA affirms that it neither has nor seeks the ability to remove or edit what information is made available on social media platforms. CISA makes no recommendations about how the information it is sharing should be handled or used by social media companies. Additionally, CISA will not take any action, favorable or unfavorable, toward social media companies based on decisions about how or whether to use this information.

From: Misinformation Reports <misinformation@cisecurity.org>
Sent: Tuesday, October 27, 2020 4:07 PM
To: tips@2020partnership.atlassian.net; Misinformation Reports <misinformation@cisecurity.org>; Scully, Brian <brian.scully1@cisa.dhs.gov>; CFITF <cfitf@hq.dhs.gov>; CISA Central <central@cisa.dhs.gov>
Subject: Case #CIS-MIS000075: Misinformation tweet regarding re-voting

CAUTION: This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

Misinformation tweet regarding re-voting

Begin forwarded message:

From: "Augino, Lori" <lori.augino@sos.wa.gov>
Date: October 27, 2020 at 4:00:35 PM EDT
To: Misinformation Reports <misinformation@cisecurity.org>
Cc: "Zabel, Kylee" <kylee.zabel@sos.wa.gov>
Subject: Misinfo - tweet from President

In Washington, you cannot change your mind and re-vote.

From:

[[mailto:](#)]

Sent: Tuesday, October 27, 2020 12:52 PM
To: Elections - Public <elections@sos.wa.gov>
Subject: Disinformation

I'm reporting this disinformation about the elections. Please take steps to stop it, and correct it publicly. Thanks.

Federal Way, WA



.....

This message and attachments may contain confidential information. If it appears that this message was sent to you by mistake, any retention, dissemination, distribution or copying of this message and attachments is strictly prohibited. Please notify the sender immediately and permanently delete the message and any attachments.

.....

DEFENDANTS' EXHIBIT 109:

From: Scully, Brian [brian.scully1@cisa.dhs.gov]
Sent: 9/26/2020 7:20:22 PM
To: Stacia Cardille [scardille@twitter.com]
CC: Lisa Roman [lroman@twitter.com]
Subject: Re: FW: Reporting Twitter post with misinformation on recent Colorado mailing

Thanks for quick response Stacia.

Brian

Brian Scully
DHS Countering Foreign Interference Task Force
National Risk Management Center
(202) 450-8046
brian.scully1@cisa.dhs.gov

From: Stacia Cardille <scardille@twitter.com>
Sent: Saturday, September 26, 2020 7:12:37 PM
To: Scully, Brian <brian.scully1@cisa.dhs.gov>
Cc: Lisa Roman <lroman@twitter.com>
Subject: Re: FW: Reporting Twitter post with misinformation on recent Colorado mailing

CAUTION: This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

Hi Brian, our enforcement teams reviewed the reports and found the Tweets to not be in violation of our policies. We will not take action on these Tweets. Thank you.

On Sat, Sep 26, 2020 at 4:57 PM Scully, Brian <brian.scully1@cisa.dhs.gov> wrote:

Hi Stacia and Lisa,

Please see the below reporting from the Colorado Secretary of State's Office. Please let me know if you have any questions or if you require any additional information.

Thanks,
Brian

The Cybersecurity and Infrastructure Security Agency (CISA) of the U.S. Department of Homeland Security (DHS) is not the originator of this information. CISA is forwarding this information, unedited, from its originating source – this information has not been originated or generated by CISA. This information may also be shared with law enforcement or intelligence agencies.

CISA affirms that it neither has nor seeks the ability to remove or edit what information is made available on social media platforms. CISA makes no recommendations about how the information it is sharing should be handled or used by social media companies. Additionally, CISA will not take any action, favorable or unfavorable, toward social media companies based on decisions about how or whether to use this information.

From: Trevor Timmons <Trevor.Timmons@SOS.STATE.CO.US>
Sent: Saturday, September 26, 2020 4:13 PM
To: Central Cyber <central.cyber@cisa.dhs.gov>; soc@cisecurity.org; CIAC Security <cdps_ciac_security@state.co.us>
Cc: Scully, Brian <brian.scully1@cisa.dhs.gov>; Masterson, Matthew <Matthew.Masterson@cisa.dhs.gov>; Hale, Geoffrey <Geoffrey.Hale@cisa.dhs.gov>; Snell, Allison <Allison.Snell@cisa.dhs.gov>; Ian Rayder <Ian.Rayder@SOS.STATE.CO.US>; Melissa Kessler <Melissa.Kessler@SOS.STATE.CO.US>; Judd Choate <Judd.Choate@SOS.STATE.CO.US>; Hilary Rudy <Hilary.Rudy@SOS.STATE.CO.US>; Nathan Blumenthal <Nathan.Blumenthal@SOS.STATE.CO.US>; Aaron Hayman (Temporary) <Aaron.Hayman@SOS.STATE.CO.US>; Josh Craven <Josh.Craven@SOS.STATE.CO.US>; Craig Buesing <Craig.Buesing@SOS.STATE.CO.US>; Rich Schliep <Rich.Schliep@SOS.STATE.CO.US>; Jeff Oliver <Jeff.Oliver@SOS.STATE.CO.US>; Dwight Shellman <Dwight.Shellman@SOS.STATE.CO.US>
Subject: Reporting Twitter post with misinformation on recent Colorado mailing
Importance: High

CAUTION: This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

Afternoon,

We'd like Twitter to review recent posts from a Denver news channel that contains misinformation about a recent mailing from the Colorado Secretary of State's office:

<https://twitter.com/CBSDenver/status/1309652042021912576>

<https://twitter.com/CBS4Shaun/status/1309660915311079424>

The posts have been highlighted as containing false information by personnel from our office, other media sources, and others. At best, we'd suggest they be removed as promoting inaccurate and false information. At a minimum, we'd request they be labeled as "false".

For rapid contact, I'm reachable by text or Signal at 303-917-5880.

- Trevor



Trevor Timmons

Chief Information Officer | Department of State

303.860.6946 (direct)

303.894.2200 (office)

trevor.timmons@sos.state.co.us

[1700 Broadway, Suite 200](#)

[Denver, CO 80290](#)

DEFENDANTS' EXHIBIT 110:

From: Scully, Brian [/O=EXCHANGELABS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=7CA10604AEE04B1DAB53DC9F884130BD-SCULLY, BRI]
Sent: 5/12/2020 9:20:03 AM
To: Stacia Cardille [scardille@twitter.com]
CC: Lisa Roman [lroman@twitter.com]
Subject: RE: FW: Twitter

Thanks Stacia.

Brian

From: Stacia Cardille <scardille@twitter.com>
Sent: Tuesday, May 12, 2020 5:06 AM
To: Scully, Brian <brian.scully1@cisa.dhs.gov>
Cc: Lisa Roman <lroman@twitter.com>
Subject: Re: FW: Twitter

CAUTION: This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

Thank you, Brian. Our internal review of account data indicates it is not suspicious.

Thanks for your help.
Stacia

On Fri, May 8, 2020 at 4:40 PM Stacia Cardille <scardille@twitter.com> wrote:

Thanks, Brian, we will escalate it internally.

Have a great weekend, and look forward to speaking on Monday.

On Fri, May 8, 2020 at 4:39 PM Scully, Brian <brian.scully1@cisa.dhs.gov> wrote:

Hi Lisa and Stacia,

Please see below reporting we received from Dominion Voting. As you know, DHS will not ask you to take any specific action, but simply want to make sure you have awareness and information about possible disinformation or other problems on your platform. Please let me know if you have any questions or comments.

Thanks,
Brian

From: Masterson, Matthew <Matthew.Masterson@cisa.dhs.gov>
Sent: Friday, May 8, 2020 3:06 PM
To: Scully, Brian <brian.scully1@cisa.dhs.gov>
Cc: Hale, Geoffrey <Geoffrey.Hale@cisa.dhs.gov>; Snell, Allison <Allison.Snell@cisa.dhs.gov>; McKinnis, Seth <seth.mckinnis@cisa.dhs.gov>
Subject: FW: Twitter

Brian,

See below from Dominion Voting regarding a suspicious twitter account. They requested that if we hear anything back we please let them know.

Matthew V. Masterson
Senior Cybersecurity Advisor
Department of Homeland Security
Cybersecurity & Infrastructure Security Agency (CISA)
(202)309-1585
Matthew.Masterson@hq.dhs.gov

From: Kay Stimson <kay.stimson@dominionvoting.com>
Sent: Friday, May 8, 2020 2:31 PM
To: Hale, Geoffrey <Geoffrey.Hale@cisa.dhs.gov>; Masterson, Matthew <Matthew.Masterson@cisa.dhs.gov>
Subject: Twitter

CAUTION: This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

Matt and Geoff,

For awareness, Dominion's corporate Twitter account picked up a new follower today who raised an alert: @elbotxi (aka Ziggy Stardust).

<https://twitter.com/elbotxi>

Due to the Anonymous reference in the profile header complete with Guy Fawkes mask, we are flagging it mainly as a precaution. We noticed Ziggy is also following ScytL.

No unusual IT activity to report.

Regards,
Kay

KAY STIMSON | VP, GOVERNMENT AFFAIRS
DOMINION VOTING SYSTEMS

866-654-VOTE (8683) | [DOMINIONVOTING.COM](https://www.dominionvoting.com)

DEFENDANTS' EXHIBIT 111:

From: Scully, Brian [/O=EXCHANGELABS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=7CA10604AEE04B1DAB53DC9F884130BD-SCULLY, BRI]
Sent: 11/11/2020 9:57:01 PM
To: Todd O'Boyle [toboyle@twitter.com]
CC: CFITF [cfitf@hq.dhs.gov]; CISA Central [central@cisa.dhs.gov]; Misinformation Reports [misinformation@cisecurity.org]; Stacia Cardille [scardille@twitter.com]; tips@2020partnership.atlassian.net
Subject: RE: CIS-MIS000197 - allegations of election fraud in Kentucky

Thanks Todd. We'll remove Neema and the Gov't emails from the distro.

Regards,
Brian

From: Todd O'Boyle <toboyle@twitter.com>
Sent: Wednesday, November 11, 2020 9:56 PM
To: Scully, Brian <brian.scully1@cisa.dhs.gov>
Cc: CFITF <cfitf@hq.dhs.gov>; CISA Central <central@cisa.dhs.gov>; Misinformation Reports <misinformation@cisecurity.org>; Stacia Cardille <scardille@twitter.com>; tips@2020partnership.atlassian.net
Subject: Re: CIS-MIS000197 - allegations of election fraud in Kentucky

CAUTION: This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

This tweet was not determined to violate our civic integrity policy.

On Wed, Nov 11, 2020 at 9:30 PM Todd O'Boyle <toboyle@twitter.com> wrote:

Hi Brian -
Thanks for getting in touch, we will escalate this report.

By the way, now that we are through the election week no need to email these reports to gov@twitter. To get the most reliable response email myself and Stacia.

Warmest,
Todd

DEFENDANTS' EXHIBIT 112:



An official website of the United States government

[Here's how you know](#) ▾



**CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY**

Menu

AMERICA'S CYBER DEFENSE AGENCY

SHARE:    



Election Security Rumor vs. Reality

Rumor vs. Reality is designed to address common disinformation narratives by providing accurate information related to elections.



Looking for information on state-specific election security efforts or additional FAQs? Check out the #TrustedInfo2022

<<https://www.nass.org/initiatives/trustedinfo>> page from the National Association of Secretaries of State (NASS) and the Election FAQs

<<https://www.nased.org/faqs>> page from the National Association of State Election Directors (NASED).

State, local, and territorial election officials work year-round to prepare for and administer elections, implementing a wide range of security measures and serving as authoritative sources of official government information on elections for their voters. While important commonalities exist across and within states, each state, local, and territorial election jurisdiction administers its elections under a unique legal and procedural framework using varying systems and infrastructure. The differences and complexity introduced by this decentralization can lead to uncertainty in the minds of voters; uncertainty that can be exploited by malicious actors.

Complementing election officials' voter education and civic literacy efforts, this page seeks to inform voters and help them build resilience against foreign influence operations and disinformation narratives about election infrastructure. Rumor vs. Reality is designed to provide accurate and reliable information that relate broadly to the security of election infrastructure and related processes.

This page is not intended to address jurisdiction-specific claims. Instead, this resource addresses election security rumors by describing common and generally applicable protective processes, security measures, and legal requirements designed to deter, detect, and protect against significant security threats related to election infrastructure and processes.

Pre-Election	+
Election Day	+
Post-Election	+

Publication

Rumor vs. Realidad </resources-tools/resources/rumor-vs-realidad>

PUBLICATION

November 4, 2022: El material de CISA "Rumor vs. Realidad" está ahora disponible en español. Encuéntrelo en @CISAgov y compártalo en Twitter para crear conciencia acerca de la información electoral exacta y de las narrativas electorales comunes de MD

Download File (PDF, 497.26 KB)

#TrustedInfo2022

Looking for information on state-specific election security efforts?

Check out the [#TrustedInfo2022](https://www.nass.org/initiatives/trustedinfo) page from the National Association of Secretaries of State (NASS).

LEARN MORE

<https://www.nass.org/initiatives/trustedinfo>

ELECTION SECURITY

VIEW MORE INFORMATION

[/to
pics/
elec
tion-
secu
rity](#)

[Return to top](#)

Topics

Spotlight

Resources & Tools

News & Events

Careers

About



**CYBERSECURITY &
INFRASTRUCTURE**



SECURITY AGENCY



CISA Central

888-282-0870

Central@cisa.dhs.gov

CISA.gov

An official website of the U.S. Department of Homeland Security

[About CISA </about>](#)

[Accessibility <https://www.dhs.gov/accessibility>](https://www.dhs.gov/accessibility)

[Budget and Performance](#)
<https://www.dhs.gov/performance-financial-reports>

[DHS.gov <https://www.dhs.gov>](https://www.dhs.gov)

[FOIA Requests <https://www.dhs.gov/foia>](https://www.dhs.gov/foia)

[No FEAR Act </cisa-no-fear-act-reporting>](#)

[Office of Inspector General](#)
<https://www.oig.dhs.gov/>

[Privacy Policy </privacy-policy>](#)

[Subscribe](#)

[The White House <https://www.whitehouse.gov/>](https://www.whitehouse.gov/)

[USA.gov <https://www.usa.gov/>](https://www.usa.gov/)

[Website Feedback </forms/feedback>](#)

DEFENDANTS' EXHIBIT 113:

Social Media Resources

- **Community Testing Events**
- **Resources for Public Use**
- **Generic Graphics**
- **Rumor Control Series**
- **Quotation Graphics**
- **Photos**

Below are a variety of social media resources for your use. Note, much of the copy included under each header for that set of content is based on the original post. You may want to verify the accuracy of the information in the post before use. Copy may not be included to correspond with all graphics. If you have questions related to any of these items, contact Megan Hopkins at **megan.hopkins@health.mo.gov** (**mailto:megan.hopkins@health.mo.gov**).

To use an image, click on the image name. It will open the image, and you can right click on the image to save it.

Community Testing Events

- **EXAMPLE Community Testing Event Post**
(<https://health.mo.gov/living/healthcondiseases/communicable/novel-coronavirus-lpha/social-media-resources/community-testing-events/example.docx>)

Central Missouri Area

Kansas City Missouri Area

Northwest Missouri Area

Northeast Missouri Area

St. Louis Missouri Area

Southeast Missouri Area

Southwest Missouri Area

Resources for Public Use

- **Posts to Accompany Resources for Public Use**
(<https://health.mo.gov/living/healthcondiseases/communicable/novel-coronavirus-lpha/social-media-resources/resources-public-use/posts.docx>)
- **Battelle (Facebook)**(<https://health.mo.gov/living/healthcondiseases/communicable/novel-coronavirus-lpha/social-media-resources/resources-public-use/Battelle-Facebook.png>)

- **Battelle System Pick Up and Drop Off sites**(<https://health.mo.gov/living/healthcondiseases/communicable/novel-coronavirus-lpha/social-media-resources/resources-public-use/Battelle-System-Pick-Up-and-Drop-Off-Sites.jpg>)
- **Battelle (Twitter)**(<https://health.mo.gov/living/healthcondiseases/communicable/novel-coronavirus-lpha/social-media-resources/resources-public-use/Battelle-Twitter.png>)
- **PPE (Facebook)**(<https://health.mo.gov/living/healthcondiseases/communicable/novel-coronavirus-lpha/social-media-resources/resources-public-use/PPE-Facebook.png>)
- **PPE (Twitter)**(<https://health.mo.gov/living/healthcondiseases/communicable/novel-coronavirus-lpha/social-media-resources/resources-public-use/PPE-Twitter.png>)

Generic Graphics

- **Post Content for SOME Graphics**
(<https://health.mo.gov/living/healthcondiseases/communicable/novel-coronavirus-lpha/social-media-resources/generic-graphics/post-content-for-SOME-Graphics.docx>)
- **Closer look at COVID**(<https://health.mo.gov/living/healthcondiseases/communicable/novel-coronavirus-lpha/social-media-resources/generic-graphics/Closer-Look-at-COVID.jpg>)
- **COVID Cleaning Supplies**(<https://health.mo.gov/living/healthcondiseases/communicable/novel-coronavirus-lpha/social-media-resources/generic-graphics/COVID-Cleaning-Supplies.jpg>)
- **COVID Cloth Face Covering Guidance**(<https://health.mo.gov/living/healthcondiseases/communicable/novel-coronavirus-lpha/social-media-resources/generic-graphics/COVID-Cloth-Face-Covering-Guidance.jpg>)
- **COVID Do the Five**(<https://health.mo.gov/living/healthcondiseases/communicable/novel-coronavirus-lpha/social-media-resources/generic-graphics/COVID-Do-the-Five.jpg>)
- **COVID Facebook Cover Photo**(<https://health.mo.gov/living/healthcondiseases/communicable/novel-coronavirus-lpha/social-media-resources/generic-graphics/COVID-Facebook-Cover-Photo.jpg>)
- **COVID Long Term Care Facilities**(<https://health.mo.gov/living/healthcondiseases/communicable/novel-coronavirus-lpha/social-media-resources/generic-graphics/COVID-Long-Term-Care-Facilities.jpg>)
- **COVID Mental Health**(<https://health.mo.gov/living/healthcondiseases/communicable/novel-coronavirus-lpha/social-media-resources/generic-graphics/COVID-Mental-Health.jpg>)
- **COVID N95 Mask**(<https://health.mo.gov/living/healthcondiseases/communicable/novel-coronavirus-lpha/social-media-resources/generic-graphics/COVID-N95-mask.jpg>)
- **COVID N95 Mask with Stethoscope**(<https://health.mo.gov/living/healthcondiseases/communicable/novel-coronavirus-lpha/social-media-resources/generic-graphics/COVID-N95-mask-with-stethoscope.jpg>)
- **COVID Plasma Donation**(<https://health.mo.gov/living/healthcondiseases/communicable/novel-coronavirus-lpha/social-media-resources/generic-graphics/COVID-Plasma-Donation.jpg>)
- **COVID Reliable Information Sources**(<https://health.mo.gov/living/healthcondiseases/communicable/novel-coronavirus-lpha/social-media-resources/generic-graphics/COVID-Reliable-Information-Sources.jpg>)
- **COVID Rumor Control**(<https://health.mo.gov/living/healthcondiseases/communicable/novel-coronavirus-lpha/social-media-resources/generic-graphics/COVID-Rumor-Control.jpg>)

- **COVID Social Distancing**(<https://health.mo.gov/living/healthcondiseases/communicable/novel-coronavirus-lpha/social-media-resources/generic-graphics/COVID-Social-Distancing.jpg>)
- **COVID Testing Update (Nurses)**
(<https://health.mo.gov/living/healthcondiseases/communicable/novel-coronavirus-lpha/social-media-resources/generic-graphics/COVID-Testing-Update-Nurses.jpg>)
- **COVID Testing Updates**(<https://health.mo.gov/living/healthcondiseases/communicable/novel-coronavirus-lpha/social-media-resources/generic-graphics/COVID-Testing-Updates.jpg>)
- **Risk of Transmission and Mask Wearing** (social-media-resources/generic-graphics/risk-transmission-masks.png)
- **Show Me Strong Recovery - 4 Pillars**(<https://health.mo.gov/living/healthcondiseases/communicable/novel-coronavirus-lpha/social-media-resources/generic-graphics/ShowMeStrongRecovery-4-Pillars.jpg>)
- **Symptoms Comparison**(<https://health.mo.gov/living/healthcondiseases/communicable/novel-coronavirus-lpha/social-media-resources/generic-graphics/Symptoms-Comparison.jpg>)

Rumor Control Series

- **Rumor Control Posts**
(<https://health.mo.gov/living/healthcondiseases/communicable/novel-coronavirus-lpha/social-media-resources/rumor-control-series/rumor-control-posts.docx>)
- **5G Technology**(<https://health.mo.gov/living/healthcondiseases/communicable/novel-coronavirus-lpha/social-media-resources/rumor-control-series/5G-Technology.jpg>)
- **Additional Symptoms**(<https://health.mo.gov/living/healthcondiseases/communicable/novel-coronavirus-lpha/social-media-resources/rumor-control-series/Additional-Symptoms.jpg>)
- **Antibiotics**(<https://health.mo.gov/living/healthcondiseases/communicable/novel-coronavirus-lpha/social-media-resources/rumor-control-series/Antibiotics.jpg>)
- **Chloroquine Phosphate**(<https://health.mo.gov/living/healthcondiseases/communicable/novel-coronavirus-lpha/social-media-resources/rumor-control-series/Chloroquine-Phosphate.jpg>)
- **Cloth Face Coverings**(<https://health.mo.gov/living/healthcondiseases/communicable/novel-coronavirus-lpha/social-media-resources/rumor-control-series/Cloth-Face-Coverings.jpg>)
- **Contact Lenses**(<https://health.mo.gov/living/healthcondiseases/communicable/novel-coronavirus-lpha/social-media-resources/rumor-control-series/Contact-Lenses.jpg>)
- **Emergency Rooms**(<https://health.mo.gov/living/healthcondiseases/communicable/novel-coronavirus-lpha/social-media-resources/rumor-control-series/Emergency-Rooms.jpg>)
- **Flu Shot**(<https://health.mo.gov/living/healthcondiseases/communicable/novel-coronavirus-lpha/social-media-resources/rumor-control-series/Flu-Shot.jpg>)
- **Hand Dryers**(<https://health.mo.gov/living/healthcondiseases/communicable/novel-coronavirus-lpha/social-media-resources/rumor-control-series/Hand-Dryers.jpg>)
- **Incubation Period**(<https://health.mo.gov/living/healthcondiseases/communicable/novel-coronavirus-lpha/social-media-resources/rumor-control-series/Incubation-Period.jpg>)
- **Mail and Packages**(<https://health.mo.gov/living/healthcondiseases/communicable/novel-coronavirus-lpha/social-media-resources/rumor-control-series/Mail-and-Packages.jpg>)
- **Pain Relievers**(<https://health.mo.gov/living/healthcondiseases/communicable/novel-coronavirus-lpha/social-media-resources/rumor-control-series/Pain-Relievers.jpg>)

- **Pets**(<https://health.mo.gov/living/healthcondiseases/communicable/novel-coronavirus-lpha/social-media-resources/rumor-control-series/Pets.jpg>)
- **Pneumonia Vaccine**(<https://health.mo.gov/living/healthcondiseases/communicable/novel-coronavirus-lpha/social-media-resources/rumor-control-series/Pneumonia-Vaccine.jpg>)
- **Salt Water**(<https://health.mo.gov/living/healthcondiseases/communicable/novel-coronavirus-lpha/social-media-resources/rumor-control-series/Salt-Water.jpg>)
- **Silver Products**(<https://health.mo.gov/living/healthcondiseases/communicable/novel-coronavirus-lpha/social-media-resources/rumor-control-series/Silver-Products.jpg>)
- **Surface Viability**(<https://health.mo.gov/living/healthcondiseases/communicable/novel-coronavirus-lpha/social-media-resources/rumor-control-series/Surface-Viability.jpg>)
- **Zinc Supplements**(<https://health.mo.gov/living/healthcondiseases/communicable/novel-coronavirus-lpha/social-media-resources/rumor-control-series/Zinc-Supplements.jpg>)

Quotation Graphics

- **Quotations** (<https://health.mo.gov/living/healthcondiseases/communicable/novel-coronavirus-lpha/social-media-resources/quotation-graphics/quotations.docx>)
- **Outdoors is Open - Pauley**
Quote(<https://health.mo.gov/living/healthcondiseases/communicable/novel-coronavirus-lpha/social-media-resources/quotation-graphics/outdoors-is-open-pauley-quote.png>)
- **Physical Mental Health - Pauley**
Quote(<https://health.mo.gov/living/healthcondiseases/communicable/novel-coronavirus-lpha/social-media-resources/quotation-graphics/physical-mental-health-pauley-quote.png>)
- **Trails Open - Pauley**
Quote(<https://health.mo.gov/living/healthcondiseases/communicable/novel-coronavirus-lpha/social-media-resources/quotation-graphics/trails-open-pauley-quote.png>)

Photos

- **COVID Hotline**(<https://health.mo.gov/living/healthcondiseases/communicable/novel-coronavirus-lpha/social-media-resources/photos/covid-hotline.jpg>)

Rumor Control

Graphic Title	Original Post: Some of these are a few months old, so verify information before posting.
5G Technology	<p>A CLOSER LOOK AT COVID: Can 5G technology spread COVID-19? Short answer: absolutely not. Viruses cannot travel on radio waves or mobile networks, and 5G does not suppress your immune system. COVID-19 is spread through respiratory droplets when an infected person coughs, sneezes or speaks. People can also be infected by touching a contaminated surface and then their eyes, mouth or nose.</p> <p>To learn more about what you can do to protect you and your family from COVID-19, visit Health.Mo.Gov/coronavirus.</p>
Additional Symptoms	<p>A CLOSER LOOK AT COVID: Is losing your sense of smell or taste a symptom of COVID-19? Short answer: yes. Late last week, the CDC named six new symptoms of COVID-19 infection. People with COVID-19 have experienced a wide range of symptoms, ranging from mild symptoms to severe illness.</p> <p>The updated list of symptoms includes:</p> <ul style="list-style-type: none"> - Fever - Cough - Shortness of breath or difficulty breathing - Chills - Repeated shaking with chills - Muscle pain - Headache - Sore throat - New loss of taste or smell <p>To learn more from the CDC, visit https://www.cdc.gov/coronavirus/2019-ncov/symptoms-testing/symptoms.html. To learn more about what you can do to protect you and your family from COVID-19, visit Health.Mo.Gov/coronavirus.</p>
Antibiotics	<p>A CLOSER LOOK AT COVID: Are antibiotics effective against COVID-19? Short answer: no. Antibiotics attack bacteria by preventing them from reproducing. COVID-19 is caused by a virus which has no vaccine or proven treatment available. Antibiotics like azithromycin may be effective in treating bacterial infections that are caused by COVID-19 complications, but they do not directly attack the COVID-19 virus. As always, antibiotics and any other medications should be used only at the direction and advice of medical professionals.</p> <p>To learn more about what you can do to protect you and your family from COVID-19, visit Health.Mo.Gov/coronavirus.</p>
Chloroquine Phosphate	<p>A CLOSER LOOK AT COVID: Does the chloroquine phosphate I can purchase online treat COVID-19 symptoms? Short answer: definitely not, please don't ingest non-prescription chloroquine phosphate. Chloroquine phosphate, when used without a prescription and supervision of a healthcare provider, can cause serious health consequences, including death. Currently, chloroquine phosphate is being studied and evaluated as treatment for COVID-19 and was just approved by the FDA this week under emergency authority for short-term use by doctors to treat COVID-19 patients. Our team urges patients to proceed with caution before believing rumors like this one</p>

	<p>related to COVID-19.</p> <p>To learn more about what you can do to protect you and your family from COVID-19, visit Health.Mo.Gov/coronavirus.</p>
Cloth Face Coverings	<p>A CLOSER LOOK AT COVID: Did you know cloth face coverings are not meant to protect the wearer, but rather entire communities? It's true. Cloth mask is a way to contain respiratory secretions right at the source. They are meant to serve as a complimentary measure as we continue social distancing, good hygiene and enhanced cleaning efforts.</p> <p>To learn more about what you can do to protect you and your family from COVID-19, visit Health.Mo.Gov/coronavirus.</p>
Contact Lenses	<p>A CLOSER LOOK AT COVID: Is it true that I shouldn't wear glasses instead of contacts to protect my eyes from COVID-19? Short answer: contacts are still safe to wear, but it may very slightly reduce your chances of being infected. The American Academy of Ophthalmology pointed out last week that wearing glasses may act as a literal shield between your eyes and respiratory droplets from a contagious individual. It may also discourage you from naturally touching your eyes, which has been a primary hygiene recommendation from experts for months. However, Missourians should not be afraid to wear contacts as prescribed by their optometrist.</p> <p>To learn more about what you can do to protect you and your family from COVID-19, visit Health.Mo.Gov/coronavirus.</p>
Emergency Rooms	<p>A CLOSER LOOK AT COVID: Are emergency rooms still safe? Short answer: yes, if you are experiencing a health emergency, we urge you to head to the emergency room. Your experience may look a little different as hospitals and emergency rooms implement social distancing measures, but you should not be afraid to seek emergency medical care.</p> <p>To view the Show Me Strong website, visit ShowMeStrong.Mo.Gov. To see what you can continue to do to protect you and your family from COVID-19, visit Health.Mo.Gov/coronavirus.</p>
Flu Shot	<p>A CLOSER LOOK AT COVID: Is it true that patients who had a flu shot have been receiving false positive test results. Short answer: absolutely not. A history of receiving the influenza immunization does not make patients more likely to test positive for COVID-19. The flu vaccine doesn't include any of the coronaviruses and doesn't create any "viral interferences" for COVID-19 patients.</p> <p>To learn more about what you can do to protect you and your family from COVID-19, visit Health.Mo.Gov/coronavirus.</p>
Hand Dryers	<p>A CLOSER LOOK AT COVID: Are hand dryers effective in killing COVID-19? Short answer: no. Hand dryers, like those found in public restrooms, are not effective in killing the coronavirus. To protect yourself and others, you should frequently wash your hands with soap and water for at least 20 seconds. If soap and water are not available, use hand sanitizer that contains at least 60% alcohol. To learn more about what you can do to protect you and your family from COVID-19, visit Health.Mo.Gov/coronavirus.</p>
Incubation Period	<p>A CLOSER LOOK AT COVID: Is it true that it may take days for COVID-19 patients to develop symptoms? Short answer: yes, it is true. The incubation period of COVID-19 is believed to be between 1-14 days, with the median number of days being 5. This doesn't necessarily mean that patients are</p>

	<p>always contagious prior to showing symptoms, but pre-symptomatic contagious patients are being observed in some communities. This is why it's so important for us all to stay home when possible.</p> <p>To learn more about what you can do to protect you and your family from COVID-19, visit Health.Mo.Gov/coronavirus.</p>
Mail and Packages	<p>A CLOSER LOOK AT COVID: Is it true that I can get COVID-19 from mail and shipped packages? Short answer: it's unlikely. Although the virus can survive for a short period on some surfaces, it is unlikely to be spread from products or packaging that are shipped over a period of days or weeks at ambient temperatures.</p> <p>To learn more about what you can do to protect you and your family from COVID-19, visit Health.Mo.Gov/coronavirus.</p>
Pain Relievers	<p>A CLOSER LOOK AT COVID: Is it true that ibuprofen makes COVID-19 symptoms worse? Short answer: no. Physicians around the world have questioned the claim that ibuprofen is dangerous for coronavirus patients. Ibuprofen is an effective pain reliever, fever reducer and anti-inflammatory that has been available for decades and is still supported by the World Health Organization (WHO). As always, if you have questions or concerns, we encourage you to reach out to your healthcare provider for advice.</p> <p>To learn more about what you can do to protect you and your family from COVID-19, visit Health.Mo.Gov/coronavirus.</p>
Pets	<p>A CLOSER LOOK AT COVID: Can my pets get infected with the COVID-19 virus? We are still learning about this virus, and it appears that in some rare situations, people can spread the virus to animals. Some infected animals may become sick while others do not. CDC is not aware of any animal deaths in the United States due to infection with this virus. At this time, the risk of animals spreading COVID-19 to people is considered to be low. Currently, the CDC, U.S. Department of Agriculture and American Veterinary Medical Association (AVMA) agree there is no need to routinely test companion animals for COVID-19.</p> <p>If you are sick with COVID-19, it's important to practice good hygiene, like handwashing, when interacting closely with your pets or other animals, just as you would when interacting with people.</p> <p>To learn more about what you can do to protect you and your family from COVID-19, visit Health.Mo.Gov/coronavirus.</p>
Pneumonia Vaccine	<p>A CLOSER LOOK AT COVID: Do pneumonia vaccines protect against COVID-19? Short answer: no. It is possible that COVID-19 patients will have secondary complications like pneumonia; however, the vaccines for those infections are not effective in preventing the novel coronavirus from infecting patients. COVID-19 is new and different from other viruses, so it will need its own vaccine.</p> <p>To learn more about what you can do to protect you and your family from COVID-19, visit Health.Mo.Gov/coronavirus.</p>
Salt Water	<p>A CLOSER LOOK AT COVID: Is it true that gargling salt water, vinegar or mouth wash will protect me from COVID-19 infection? Short answer: no. Out of all the rumors we've seen online related to COVID-19, this one is the furthest from reality and is not supported by any medical evidence. Save</p>

	<p>yourself some time and focus on other hygiene efforts like washing your hands frequently, avoiding touching your face, eyes and mouth, and practicing social distancing.</p> <p>To learn more about what you can do to protect you and your family from COVID-19, visit Health.Mo.Gov/coronavirus.</p>
Silver Products	<p>A CLOSER LOOK AT COVID: Does silver help develop immunity from or treat COVID-19? Short answer: absolutely not. This may seem like old news, but it is worth repeating. Don't let fraudulent marketers convince you that silver products can treat or otherwise prevent coronavirus from infecting you.</p> <p>To view the Show Me Strong website, visit ShowMeStrong.Mo.Gov. To see what you can continue to do to protect you and your family from COVID-19, visit Health.Mo.Gov/coronavirus.</p>
Surface Viability	<p>A CLOSER LOOK AT COVID: How long does coronavirus live on surfaces? Short answer: research on the virus' surface viability is brand new. Survival of COVID-19 on surfaces appears to behave like other coronaviruses. Initial studies suggest it can survive on surfaces for at least a few hours, and may survive on plastic, glass and metal for several days. Although the survival length varies under different conditions (temperature, humidity and surface type), it is a good reminder to all Missourians to regularly clean and disinfect high-touch areas like doorknobs, handles and countertops.</p> <p>To learn more about Missouri's COVID-19 response efforts, visit Health.Mo.Gov/coronavirus.</p>
Zinc Supplements	<p>A CLOSER LOOK AT COVID: Can taking zinc supplements lower your risk of contracting COVID-19? Short answer: there is no research on its effectiveness. Random trials have shown that zinc supplements can reduce the risk of certain acute respiratory infections and shorten flu-like symptoms. However, there is no data on the effectiveness of zinc supplements reducing the risk or severity of COVID-19.</p> <p>To learn more about what you can do to protect you and your family from COVID-19, visit Health.Mo.Gov/coronavirus.</p>

DEFENDANTS' EXHIBIT 114:



Understanding Election Security

No single
point of
access



There are 116 election jurisdictions in Missouri, each with their own voting system. That means there is no single voting system or single point of access.

Not
connected
to internet



Voting machines are not connected to the internet, so they can't be hacked from the internet.

Voting
machine
paper trail



Every single voting machine in Missouri is required to produce a paper audit trail.

Bipartisan
counting of
absentees

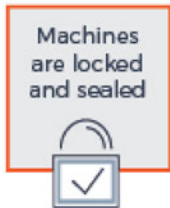


When absentee ballots are processed, they are counted by a bipartisan team.

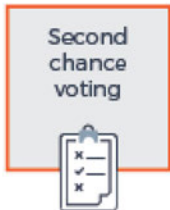
Public
testing of
machines



Voting machines are publicly tested both before and after election day.



Once checked for accuracy, election equipment is locked and sealed to prohibit any tampering with the equipment on election day.



All voting machines in Missouri are required to give the voter a second chance to ensure the ballot is marked correctly.



Election results are audited by local election officials before any results are certified.

Updates

In 2018, the Missouri Secretary of State's Office successfully obtained a federal grant in the amount of \$7.2 million through the Help America Vote Act (HAVA). The office has laid the groundwork to spend those funds with local election authorities to improve both physical security and cyber security to further enhance the integrity of Missouri's election systems.

In January of 2018, Missouri joined ERIC, the Electronic Registration Information Center, to help maintain an accurate voter registration database. ERIC is a multistate partnership that uses a sophisticated and secure data-matching tool to improve the accuracy and efficiency of state voter registration systems. Through participation in ERIC, states can compare official data on eligible voters—such as voter and motor vehicle registrations, U.S. Postal Service addresses, and Social Security death records—to keep voter rolls more complete and up to date. ERIC is owned, managed, and funded by participating states and was formed in 2012 with assistance from The Pew Charitable Trusts. More than half of U.S. states participate in ERIC.

Knowing Election Security

Voter Pamphlet on Election Security (Election Assistance Commission)
Election Security Pamphlet

The War on Pineapple: Understanding Foreign Intelligence in 5 Steps (U.S.

Department of Homeland Security)

The War on Pineapple: Understanding Foreign Interference in 5 Steps

Social Media Bots Overview

Social Media Bots Overview

Election Security Video (Election Assistance Commission)

Election Security Video

Qualified Voting Systems in Missouri

Qualified Voting Systems in Missouri

DEFENDANTS' EXHIBIT 115:

(/)

OFFICE *of the* GOVERNOR

COVID-19 Stay at Home Order

Stay At Home Order

To further combat the spread of COVID-19 in Louisiana, Gov. Edwards issued a Stay at Home Order on March 22, directing all Louisiana residents to shelter at home and limit movements outside of their homes beyond essential needs.

Click here (</assets/Proclamations/2020/JBE-33-2020.pdf>) for the governor's official order.

On April 30, Gov. Edwards extended his stay at home order until May 15 (<https://gov.louisiana.gov/index.cfm/newsroom/detail/2479>). On May 14, Gov. Edwards signed the order moving Louisiana to Phase One. (<https://gov.louisiana.gov/news/PhaseOne>) On June 4, Gov. Edwards signed the order moving Louisiana to Phase 2. (<https://gov.louisiana.gov/index.cfm/newsroom/detail/2532>)

Click here (/assets/docs/covid/Essential-Infrastructure_fact-sheet.pdf) for a list of essential infrastructure.

Click here (</can-this-business-open/>) to find out which businesses can be open.

YOU CAN

- Go to the grocery, convenience or warehouse store
- Go to the pharmacy to pick up medications and other healthcare necessities
- Go to medical appointments (check with your doctor or provider first)
- Go to a restaurant for take-out, delivery or drive-thru
- Care for or support a friend or family member
- Take a walk, ride your bike, hike, jog and be in nature for exercise — just keep at least six feet between you and others.
- Walk your pets and take them to the veterinarian if necessary
- Help someone to get necessary supplies
- Receive deliveries from any business which delivers

YOU SHOULD NOT

- Go to work unless you are providing essential services as defined by this Order
- Visit friends and family if there is no urgent need
- Maintain less than 6 feet of distance from others when you go out
- Visit loved ones in the hospital, nursing home, skilled nursing facility or other residential care facility, except for limited exceptions as provided on the facility websites.

For businesses, the new Stay at Home order has limits on the following:

- All places of public amusement, whether indoors or outdoors, including but not limited to, locations with amusement rides, carnivals, amusement parks, water parks, trampoline parks, aquariums, zoos, museums, arcades, fairs, pool halls, children's play centers, playgrounds, theme parks, any theaters, concert and music halls, adult entertainment venues, racetracks, and other similar businesses.
- All personal care and grooming businesses, including but not limited to, barber shops, beauty salons, nail salons, spas, massage parlors, tattoo parlors, and other similar businesses.
- All malls, except for stores in a mall that have a direct outdoor entrance and exit that provide essential services and products as provided by the Cybersecurity & Infrastructure Security Agency (CISA) guidelines.

- Businesses closed to the public as listed in the order can conduct necessary activities such as payroll, cleaning services, maintenance or upkeep as necessary.
- Any business not covered by the guidance from the CISA discussed in Section 3 of the order and not ordered to temporarily close must reduce operations to continue with minimum contact with members of the public and essential employees, while requiring proper social distancing, adhering to the 10-person limitation on gathering size.
- Early learning centers and child care facilities adhering to the guidance issued by the Louisiana Department of Education and Office of Public Health may continue to operate.

Examples of Essential Worker Functions under the Cybersecurity & Infrastructure Security Agency (CISA) guidelines include:

- Healthcare workers and caregivers
- Mental health and Social Service workers
- Pharmacy employees
- Workers supporting groceries, pharmacies and other retail sales of food and beverage products
- Restaurant carryout and quick-serve food operations and food delivery employees
- Farmworkers
- Electricity and Utility Industry Employees
- Critical Manufacturing Employees (medical supply chains, energy, transportation, food, chemicals)
- Petroleum, Natural and Propane Gas Workers
- Transportation and Logistics Workers
- Communications and Information Technology Employees

What is the difference between “Safer at Home” and “social distancing”?

Safer at home is a stricter form of social distancing. Safer at home means:

- Stay home (stay unexposed and do not expose others)
- Only go out for essential services
- Stay six feet or more away from others
- Don't gather in groups

What is a Stay at Home order?

A Stay at Home order is the Governor directing people to avoid going out in public unless it is absolutely necessary.

Why is this Stay at Home order necessary?

Right now, COVID-19 is spreading rapidly throughout our state and some of our communities and, without taking additional measures, Louisiana's health care system will have more sick people than it can care for. The state is working to increase its health care capacity, but people also need to take measures to prevent the spread of this illness. Our medical community is working overtime to take care of people who are sick, but it needs help from the public to keep even more people from needing care.

When is it okay for me to leave my home?

People can leave their homes to do things like buy groceries or food, pick up medicine or go to work if their job is essential. If you have to go out, make sure you practice social distancing measures and keep 6 feet between you and the people around you. Also: people are encouraged to go outside and to stay active during this time, as long as they practice social distancing when they are around their neighbors.

What if I need to get tested for coronavirus or to go to the doctor?

People can leave their homes for medical treatment or to get testing, but they should call their health care provider or doctor before doing so for advice. Your doctor may be able to help you via telemedicine or decide if you need to be tested by asking you questions on the phone. Do not show up to a testing site without consulting a medical professional first, because you may need a doctor's order to qualify for a test. Unless it is an emergency, do not go to a health care facility without calling first, because you may put yourself at risk of being exposed to COVID-19.

What businesses and jobs are considered essential?

Health care workers, public safety employees, some government workers, staff of grocery stores and restaurants and employees of some business are generally considered essential workers. Businesses like manufacturers and utilities have to continue operations to support our communities.

In general, the state of Louisiana follows guidance from the federal Cybersecurity and Infrastructure Security Agency (CISA) about what infrastructure and businesses are “critical” during the COVID-19 outbreak. For more detailed information from CISA, visit this site: <https://www.cisa.gov/identifying-critical-infrastructure-during-covid-19>

How will this order be enforced?

The state is working with local law enforcement to support the order. There have been rumors about military control or martial law being declared. These rumors are false.

Why is this order statewide? There are not a lot of cases confirmed in my area.

COVID-19 is rapidly spreading throughout the state and we know that some people do not show symptoms for 14 days, even if they are sick. Just because no one has tested positive in your community doesn’t mean that no one is sick. By enacting this Stay at Home order statewide, Gov. Edwards is working to slow the spread of COVID-19 and flatten the curve.

Is the Governor closing Louisiana’s borders and declaring martial law?

No. This is a rumor and is not based in fact. Members of Louisiana’s National Guard are deployed in Louisiana to help support local testing sites, so you may see members of the military in your community. Martial law has not been declared. Louisiana’s borders are not closed.

When is the Stay at Home order going to be lifted?

The Stay at Home order is in place until the morning of Monday, April 13, which is when schools are scheduled to re-open. Governor Edwards will re-evaluate the order before it expires to make sure that it doesn’t need to be restricted.

Where can people get more information about what the State of Louisiana is doing in response to the COVID-19 Outbreak?

The Governor’s office is constantly updating its website at gov.louisiana.gov, as is the Louisiana Department of Health at ldh.la.gov/Coronavirus (<https://jsapis/tinymce3/extension/ldh.la.gov/Coronavirus>). You can also call 211 for general information about COVID-19 and to get connected to help and resources.

CONNECT *with* the GOVERNOR

EMAIL *the*
GOVERNOR


REQUEST *of*
the GOVERNOR

APPLY *to*
SERVE




(<https://twitter.com/LouisianaGov>) (<https://www.facebook.com/LouisianaGov/>) (<https://www.instagram.com/LouisianaGov/>)

DEFENDANTS' EXHIBIT 116:



Louisiana SECRETARY OF STATE

R. KYLE ARDOYN



HOME | QUICK LINKS

SEARCH

ELECTIONS & VOTING

BUSINESS SERVICES

NOTARY & CERTIFICATIONS

HISTORICAL RESOURCES

OUR OFFICE

ELECTIONS & VOTING

Browse by Audience

+ Register to Vote

+ Vote

- Get Election Information

Search Election Dates

Polling Location Changes

Find Results & Statistics

Review Sample Ballots

Review Types of Elections

How are Candidates Elected?

Search for Candidates

Learn about Redistricting

Sign-up for Election Alerts

Review Voting Brochures & Pamphlets

Frequently Asked Questions

+ Become a Candidate

+ Find Public Officials

+ Information for Public Officials

+ Get Involved

+ Review Administration & History

+ Get Bond, Debt or Tax Costs

+ Task Forces & Study Groups

+ Get Forms & Fee Schedule

Contact Us

Click here to fill out an application to become an election worker

Home > Elections & Voting > Get Election Information > Frequently Asked Questions

Print

FREQUENTLY ASKED QUESTIONS

Click the links below to review election security measures:

- Election Day Voting
- Early Voting
- Absentee Voting

To learn what happens **before** an election, view [Frequently Asked Questions Before an Election](#).

To learn what happens **after** an election, view [Frequently Asked Questions After an Election](#).

ELECTIONS & VOTING

Browse by Audience

Register to Vote

Vote

Get Election Information

Become a Candidate

Find Public Officials

Information for Public Officials

Get Involved

Review Administration & History

Get Bond, Debt or Tax Costs

Task Forces & Study Groups

Get Forms & Fee Schedule

Contact Us

NOTARY & CERTIFICATIONS

Become a Louisiana Notary

Prepare for the Notary Exam

File Notary Documents

Search for Louisiana Notaries

Notary Education Provider Information

Become a RON Notary

Certifications

Contact Us

HISTORICAL RESOURCES

Browse by Audience

Learn about the Archives

Explore Media Archives

Research Historical Records

Managing Records

Visit Museums

About Louisiana

Contact Us

OUR OFFICE

Learn about Kyle Ardoyn

Department Overview

Find Administrative Rules

Obtain Publications

End of Life Registries

Government Entity Registries

View Solicitations

Address Confidentiality Program

Call Before You Dig

Flood Protection Authorities

Contact Us

Make a Public Records Request

Litigation Disclosure Reports

SOS Policy Against Sexual Harassment

SITE INFORMATION

Disclaimer

Accessibility

Security & Privacy

Report a Problem

[COVID-19 Resources](#)

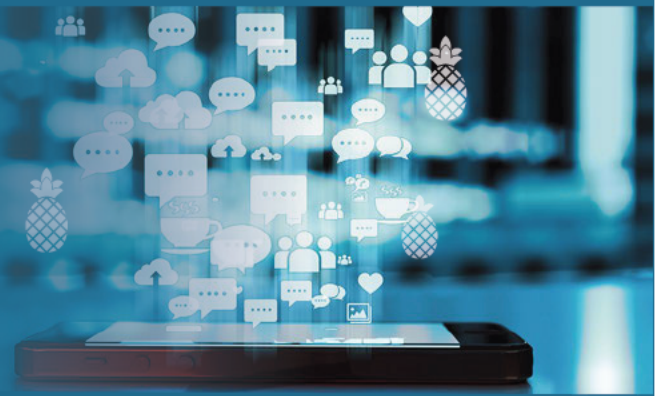
[Contact Us](#)

Free software is required to view some content on this site. If you are having problems accessing a file, click the file type below to install the necessary software:
[PDF \(Adobe Acrobat Viewer\)](#) | [DOC or DOCX \(Microsoft Word Viewer\)](#) | [XLS or XLSX \(Microsoft Excel Viewer\)](#)

© 2023 Louisiana Department of State

DEFENDANTS' EXHIBIT 117:

THE WAR ON PINEAPPLE: Understanding Foreign Interference in 5 Steps



To date, we have no evidence of Russia (or any nation) actively carrying out information operations against pizza toppings. This infographic is an ILLUSTRATION of how information operations have been carried out in the past to exploit divisions in the United States.

1. TARGETING DIVISIVE ISSUES

Foreign influencers are constantly on the lookout for opportunities to inflame hot button issues in the United States.



They don't do this to win arguments; they want to see us divided.



American Opinion is Split: Does Pineapple Belong on Pizza?

An A-list celebrity announced their dislike of pineapples on pizza, prompting a new survey. No matter how you slice it, Americans disagree on the fruit topping.

2. MOVING ACCOUNTS INTO PLACE

Building social media accounts with a large following takes time and resources, so accounts are often renamed and reused. Multiple accounts in a conversation are often controlled by the same user.



Pro Tip: Look at an account's activity history. **Genuine accounts usually have several interests and post content from a variety of sources.**

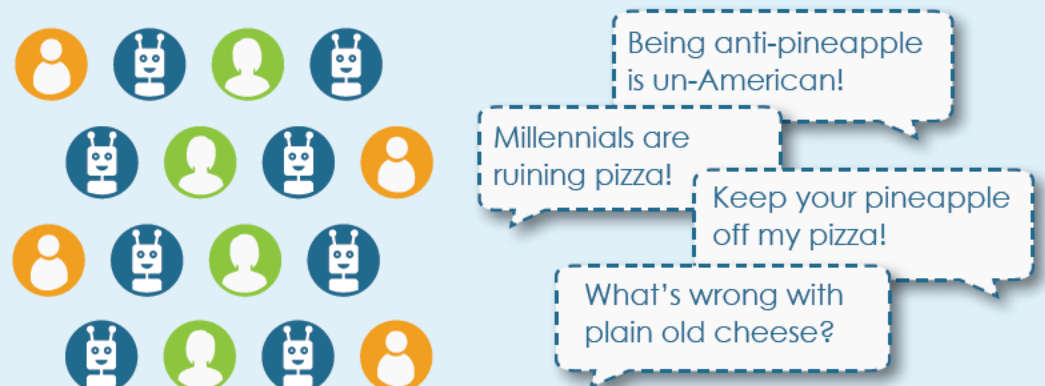


3. AMPLIFYING AND DISTORTING THE CONVERSATION

Americans often engage in healthy debate on any number of topics. Foreign influencers try to pollute those debates with bad information and make our positions more extreme by picking fights, or "trolling" people online.



Pro Tip: Trolls try to make people mad, that's it. **If it seems like an account is only aiming to raise tensions, think about whether it's worth engaging.**



4. MAKING THE MAINSTREAM

Foreign influencers "fan the flames" by creating controversy, amplifying the most extreme version of arguments on both sides of an issue. These are shared online as legitimate information sources.



Sometimes controversies make it into the mainstream and create division among Americans. **This is a foreign influencer striking gold! Their meddling is legitimized and carried to larger audiences.**



5. TAKING THE CONVERSATION INTO THE REAL WORLD

In the past, Kremlin agents have organized or funded protests to further stoke divisions among Americans. They create event pages and ask followers to come out.

What started in cyberspace can turn very real, with Americans shouting down Americans because of foreign interference.



Pro Tip: Many social media companies have increased transparency for organization accounts. **Know who is inviting you and why.**



DEFENDANTS' EXHIBIT 118:



SOCIAL MEDIA BOTS OVERVIEW

Social Media Bot programs are common and adaptable to various social media platforms across multiple venues and areas of interest. Social Media Bot usage continues to increase on various social media platforms within the United States. As Social Media Bots increase in usage and utility, malicious behavior via Social Media Bots is also likely to increase. Recent elections in 2016 and 2017 in the United States, United Kingdom, France, and Germany have drawn a spotlight on the nefarious activity of Social Media Bots.



OCIA defines Social Media Bots as programs that vary in size depending on their function, capability, and design, and can be used on social media platforms to do various useful and malicious tasks while simulating human behavior. These programs use artificial intelligence, big data analytics, and other programs or databases to imitate legitimate users posting content.

Automated Social Media Bots allow the user to establish a set of parameters using programming language within an application or program (e.g., retweet a specific hashtag every time it is posted, but not when the bot itself retweets it) which the Social Media Bot then executes without human interaction.



Semi-automated Social Media Bots allow a user to program a set of parameters but may have or require additional user interaction or a greater degree of management. These types of Social Media Bots are typically fake accounts with fake personalities and are run at least partially by humans or click farms, rather than programming language.



Common Attack Methods of Social Media Bots

- Click Farming or Like Farming** inflate fame or popularity on a website through liking or reposting of content via Click Farms, which provide fake user accounts (typically semi-automated Social Media Bots) and management of the Social Media Bots (e.g., bot herder) for purchase.
- Hashtag Hijacking** use hashtags to focus an attack (e.g., spam malicious links) on a specific audience using the same hashtag.
- Repost Storm** use a parent Social Media Bot account, or martyr Social Media Bot, to initiate an attack by reposting something, which an associated group of Social Media Bots (aka botnet) instantly reposts.

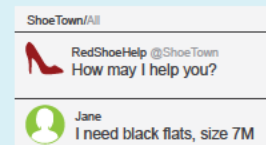
- Sleeper Bots** remain dormant for long periods of time, wake up to launch their attack of thousands of posts or retweets in a short period of time (perhaps as a Retweet Storm, or spam attack), then return to a dormant state.
- Trend Jacking and Watering Hole Attack** use top trending topics to focus on an intended audience for targeting purposes.

Social Media Bot Uses

(Below examples are fictitious)

Commercial Activity

Social Media Bots facilitate company-to-customer relations, including selling of products or services.



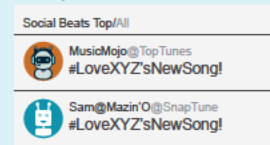
Counterterrorism and Terrorism

Social Media Bots allow for faster searching and detection of online activity by using foreign language search terms.



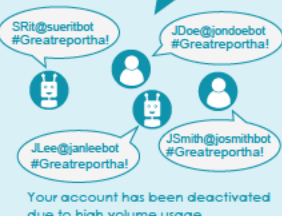
Entertainment

Social Media Bots are used on social media specifically to find, add, or create the illusion of online fame or popularity.



Harassment

Social Media Bots can be used to overwhelm the user's account to the point of deactivation.



Hate Speech

Social Media Bots can propagate hate speech on social media platforms making the subject matter appear to gain mainstream popularity.



Information Operations

The intentional spread of propaganda to sway public opinion, limit free speech, and manipulate democratic processes and elections.



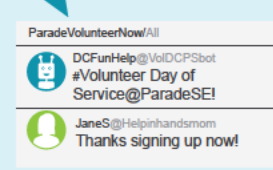
Notifications

Social Media Bots provide automated watching capabilities to capture breaking news, ideas, or events.



Social and Civic Engagement

Social Media Bots post to encourage and heighten civic engagement and participation.



Social Media Bots Signature Behaviors

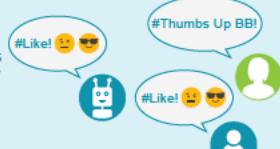
Congregation of Bots

Social Media Bots often congregate together and act with randomness making them easier to identify.



Specific Content

Social Media Bots tend to use emoticons, exclamation points, or other content in more regular patterns as compared to human users on social media.



Activity Levels

Social Media Bots often have higher levels of activity (typically automated Social Media Bots) as compared to human social media behavior.

Activity Level Comparison




Conclusion

Social Media Bots are becoming more prevalent and better at mimicking human behavior on social media platforms. As of 2017, technology companies are seeking investments and further incorporation of Social Media Bots into social media services and platforms, expanding future digital communication to provide a myriad of services as automated assistants. As Social Media Bots gain a greater foothold in social media and daily life, the potential uses for good and malicious purposes are ever expanding.

DEFENDANTS' EXHIBIT 119:



An official website of the United States government

[Here's how you know](#) 



**CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY**

Menu

AMERICA'S CYBER DEFENSE AGENCY

SHARE:    

Resources & Tools

COMMITTEE

CISA Cybersecurity Advisory Committee



The Department of Homeland Security established the Cybersecurity and Infrastructure Security Agency (CISA) Cybersecurity Advisory Committee in June of 2021 to advance CISA's cybersecurity mission and strengthen the cybersecurity of the United States. As an independent advisory body, the Committee provides strategic and actionable recommendations to the CISA Director on a range of cybersecurity issues, topics, and challenges.

Mission

Advise, consult with, report, and make recommendations to CISA on the development, refinement, and implementation of policies, programs, planning, and training pertaining to CISA's cybersecurity mission.

Committee Members

With subject matter expertise in various critical infrastructure sectors, CSAC committee members [participate in the development, refinement, and implementation of recommendations, policies, programs, planning, and training pertaining to CISA's cybersecurity mission.](#)

The Committee directs its subcommittees—established by the CISA Director as necessary—to work on specific study topics to address cybersecurity issues, including information exchange, critical infrastructure, risk management, and public and private partnerships.

Latest CSAC News and Updates

Discover recent CISA news and updates about CSAC.

[Readout from CISA's Sixth Cybersecurity Advisory Committee Meeting](#) [</news-events/news/readout-cisas-sixth-cybersecurity-](#)

[advisory-committee-meeting>](#)

MAR 21, 2023 | PRESS RELEASE

Today, the Cybersecurity and Infrastructure Security Agency (CISA) held its sixth Cybersecurity Advisory Committee meeting, the first quarterly meeting of 2023.

[Director Easterly Announces New Members to Join CISA's Cybersecurity Advisory Committee](#) [</news-events/news/director-easterly-announces-new-members-join-cisas-cybersecurity-advisory-](#)

[committee>](#)

MAR 20, 2023 | PRESS RELEASE

Today, the Cybersecurity and Infrastructure Security Agency (CISA) Director Jen Easterly announced the appointment of additional members to the CISA Cybersecurity Advisory Committee (CSAC), bringing onboard additional experts from the public and private sectors.

[Readout from CISA's Fifth Cybersecurity Advisory Committee Meeting](#) </news-events/news/readout-cisas-fifth-cybersecurity-advisory-committee-meeting>

DEC 06, 2022 | PRESS RELEASE

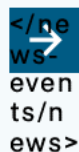
At the 5th Cybersecurity Advisory Committee (CSAC), Director Easterly led a discussion with committee members on the CSAC's strategic focus for 2023.

[CISA Holds Inaugural Meeting of New Cybersecurity Advisory Committee](#) </news-events/news/cisa-holds-inaugural-meeting-new-cybersecurity-advisory-committee>

DEC 10, 2021 | PRESS RELEASE

CISA held its first meeting for newly appointed members of the Agency's Cybersecurity Advisory Committee. Members discussed Committee objectives and initiatives, received a classified threat briefing, elected Committee leadership, and established subcommittees.

VIEW ALL CISA NEWS



CSAC Resources, Reports, and Recommendations

View CSAC's fact sheets, reports, and recommendations.

[CISA Cybersecurity Advisory Committee \(CSAC\) Fact Sheet](/resources-tools/resources/cisa-cybersecurity-advisory-committee-csac-fact-sheet)

[sheet](/resources-tools/resources/cisa-cybersecurity-advisory-committee-csac-fact-sheet)

MAR 20, 2023 | PUBLICATION

A fact sheet about the CISA Cybersecurity Advisory Committee (CSAC) and how it provides independent, strategic, and actionable consensus recommendations to the CISA Director.

[Download File \(PDF, 188.98 KB\)](#)

[CISA Cybersecurity Advisory Committee \(CSAC\) Meeting Resources](/resources-tools/resources/cisa-cybersecurity-advisory-committee-csac-meeting-resources)

[committee-csac-meeting-resources](/resources-tools/resources/cisa-cybersecurity-advisory-committee-csac-meeting-resources)

MAR 13, 2023 | MEETING AGENDAS

View the quarterly meeting agendas and summaries for each CISA Cybersecurity Advisory Meeting starting from December 2021 to present.

[View Files](#)

[Cybersecurity Advisory Committee \(CSAC\) Subcommittee Fact Sheet](/resources-tools/resources/cybersecurity-advisory-committee-csac-subcommittee-fact-sheet)

[advisory-committee-csac-subcommittee-fact-sheet](/resources-tools/resources/cybersecurity-advisory-committee-csac-subcommittee-fact-sheet)

MAR 20, 2023 | PUBLICATION

The Subcommittee Fact Sheet outlines the six established subcommittees under the Cybersecurity Advisory Committee (CSAC). Each subcommittee has been established to study various aspects of CISA's cybersecurity efforts.

[Download File \(PDF, 210.38 KB\)](#)

[2022 Cybersecurity Advisory Committee \(CSAC\) Reports and Recommendations](/resources-tools/resources/2022-cybersecurity-advisory-committee-csac-reports-and-recommendations)

[cybersecurity-advisory-committee-csac-reports-and-recommendations](/resources-tools/resources/2022-cybersecurity-advisory-committee-csac-reports-and-recommendations)

MAR 06, 2023 | PUBLICATION

View the collection of reports and recommendations published by the CISA Cybersecurity Advisory Committee.

[View Files](#)

CSAC Charter and Bylaws

View the charter and bylaws that define the Cybersecurity Advisory Committee (CSAC) mission, responsibilities, and scope.

[CISA Cybersecurity Advisory Committee \(CSAC\) Charter](/resources-tools/resources/cisa-cybersecurity-advisory-committee-csac-charter)

SEP 10, 2021 | PUBLICATION

The CISA Cybersecurity Advisory Committee (CSAC) Charter defines the committee's authority, objectives, scope of activities, duties, and other rights and privileges.

[Download File \(PDF, 266.42 KB\)](#)

CISA Cybersecurity Advisory Committee (CSAC)

Bylaws [</resources-tools/resources/cisa-cybersecurity-advisory-committee-csac-bylaws>](/resources-tools/resources/cisa-cybersecurity-advisory-committee-csac-bylaws)

AUG 04, 2021 | PUBLICATION

View the CISA Cybersecurity Advisory Committee (CSAC) Bylaws to understand the governance under which CSAC provides independent, strategic, and actionable consensus recommendations to the CISA Director.

[Download File \(PDF, 390.25 KB\)](#)

Contact

CISA_CybersecurityAdvisoryCommittee@cisa.dhs.gov

[Cybersecurity Best Practices](/topics/cybersecurity-best-practices) [</topics/cybersecurity-best-practices>](/topics/cybersecurity-best-practices)

[Critical Infrastructure Security and Resilience](/topics/critical-infrastructure-security-and-resilience) [</topics/critical-infrastructure-security-and-resilience>](/topics/critical-infrastructure-security-and-resilience)

[Partnerships and Collaboration](/topics/partnerships-and-collaboration) [</topics/partnerships-and-collaboration>](/topics/partnerships-and-collaboration)

[Cyber Threats and Advisories](/topics/cyber-threats-and-advisories) [</topics/cyber-threats-and-advisories>](/topics/cyber-threats-and-advisories)

[Return to top](#)

Topics [</topics>](/topics)

Spotlight [</spotlight>](/spotlight)

Resources & Tools [</resources-tools>](/resources-tools)

News & Events </news-events>

Careers </careers>

About </about>



**CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY**



CISA Central

888-282-0870

Central@cisa.dhs.gov

CISA.gov

An official website of the U.S. Department of Homeland Security

[About CISA </about>](#)

[Accessibility <https://www.dhs.gov/accessibility>](https://www.dhs.gov/accessibility)

[Budget and Performance](#)
<https://www.dhs.gov/performance-financial-reports>

[DHS.gov <https://www.dhs.gov>](https://www.dhs.gov)

[FOIA Requests <https://www.dhs.gov/foia>](https://www.dhs.gov/foia)

[No FEAR Act </cisa-no-fear-act-reporting>](#)

[Office of Inspector General](#)
<https://www.oig.dhs.gov/>

[Privacy Policy </privacy-policy>](#)

[Subscribe](#)

[The White House <https://www.whitehouse.gov/>](https://www.whitehouse.gov/)

[USA.gov <https://www.usa.gov/>](https://www.usa.gov/)

[Website Feedback </forms/feedback>](/forms/feedback)

DEFENDANTS' EXHIBIT 120:

UNITED STATES DEPARTMENT OF HOMELAND SECURITY
CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY
CYBERSECURITY ADVISORY COMMITTEE
CHARTER

1. Committee’s Official Designation:

Cybersecurity and Infrastructure Security Agency (CISA) Cybersecurity Advisory Committee

2. Authority:

CISA [hereinafter referred to as the “Agency”] Cybersecurity Advisory Committee is established under the *National Defense Authorization Act* for Fiscal Year 2021, P.L. 116-283 (NDAA). Pursuant to section 871(a) of the *Homeland Security Act of 2002*, 6 U.S.C. § 451(a), the Secretary of Homeland Security hereby establishes the CISA Cybersecurity Advisory Committee for the purposes set forth herein. This Committee is established in accordance with and operates under the provisions of the *Federal Advisory Committee Act* (FACA) (Title 5, United States Code, Appendix).

3. Objectives and Scope of Activities

The CISA Cybersecurity Advisory Committee shall develop, at the request of the CISA Director [hereinafter referred to as the “Director”] and incorporating guidance where applicable from the Secretary of Homeland Security [hereinafter referred to as the “Secretary”], recommendations on matters related to the development, refinement, and implementation of policies, programs, planning, and training pertaining to the cybersecurity mission of the Agency.

4. Description of Duties

The duties of the CISA Cybersecurity Advisory Committee are solely advisory in nature, as established under the *National Defense Authorization Act* for Fiscal Year 2021, P.L. 116-283 (NDAA). Pursuant to section 871(a) of the *Homeland Security Act of 2002*, 6 U.S.C. § 451(a). The CISA Cybersecurity Advisory Committee shall also submit to the Director, with a copy to the Secretary, an annual report providing information on the activities, findings, and recommendations of the Committee, including its subcommittees, for the preceding year.

5. Officials to Whom the Committee Reports

The CISA Cybersecurity Advisory Committee will advise, consult with, report to, and make independent, strategic, and actionable recommendations to the CISA Director.

6. Agency Responsible for Providing Necessary Support:

CISA shall be responsible for providing financial and administrative support to the CISA Cybersecurity Advisory Committee.

7. Estimated Cost, Compensation, and Staff Support:

The estimated annual cost of operating the CISA Cybersecurity Advisory Committee is approximately \$1,450,000, which includes travel and per diem, and other administrative expenses, and five Full-Time Equivalent employees to support the Committee.

8. Designated Federal Officer:

The Director shall appoint full-time employees of the Agency as the Designated Federal Officer (DFO) and Alternate DFOs (ADFO). The DFO or the ADFO will be responsible for setting agendas and the Committee's work activities. The DFO or the ADFO will coordinate with the Homeland Security Advisory Council's DFO [hereinafter referred to as the "HSAC"] to minimize duplication and ensure complementary work activities between both groups. The DFO or ADFO approves or calls the CISA Cybersecurity Advisory Committee and subcommittee meetings, attends all committee and subcommittee meetings, adjourns any meetings when it is determined adjournment to be in the public interest, and chairs the meeting in the absence of the designated CISA Cybersecurity Advisory Committee Chair.

9. Estimated Number and Frequency of Meetings:

CISA Cybersecurity Advisory Committee meetings will be held semiannually, at a minimum, to address matters within the scope of this Charter. Meetings may be held more frequently, or as necessary and appropriate, to address mission requirements. Meetings shall be open to the public according to the FACA unless a determination is made by the appropriate DHS official in accordance with DHS policy and directives that the meeting should be closed in accordance with Title 5, United States Code, subsection (c) of 552b. At least one meeting per year will be open to the public.

10. Duration

Continuing.

11. Termination

This charter shall be in effect for two years from the date it is filed with Congress unless sooner terminated. The charter may be renewed at the end of this two year period in accordance with section 14 of FACA (5 U.S.C. App.).

12. Membership and Designation

The Committee shall be composed of up to 35 individuals. Members are appointed by the Director. The DFO will coordinate with the DFO for the HSAC to ensure that

individuals selected for appointment to the Committee are not presently or under consideration to be members of the HSAC.

In order for the Director to fully leverage broad-ranging experience and education, the CISA Cybersecurity Advisory Committee must be diverse, with regard to professional and technical expertise, and in reflecting the diversity of the nation's people. These members shall consist of subject matter experts from diverse and appropriate professions and communities nationwide, be geographically balanced, and shall include representatives of State, local, tribal, and territorial governments and of a broad and inclusive range of industries. The CISA Director may, at their discretion, select members with a background in cybersecurity issues relevant to CISA policies, plans, and programs. Specifically, membership may, at the CISA Director's discretion, include at least one, and no more than three, representatives from the following industries recommended in the authorizing statute:

- i. Defense;
- ii. Education;
- iii. Financial services and insurance;
- iv. Healthcare;
- v. Manufacturing;
- vi. Media and entertainment;
- vii. Chemical;
- viii. Retail;
- ix. Transportation;
- x. Energy;
- xi. Information Technology;
- xii. Communications; and
- xiii. Other relevant fields identified by the Director.

The term of each member shall be two years, except that a member may continue to serve until a successor is appointed. Appointments are personal to the member and cannot be transferred to another individual or other employees of the member's organization of employment. A member may be reappointed for an unlimited number of terms. The Director may review the participation of a member of the CISA Cybersecurity Advisory Committee and remove such member any time at his/her discretion to include for violation of established responsibilities as outlined in sections III.6 and III.7 of the committee's bylaws.

Members shall serve as representatives to speak on behalf of their respective organizations

Members of the CISA Cybersecurity Advisory Committee may not receive pay or benefits from the United States Government by reason of their service on the CISA Cybersecurity Advisory Committee.

13. Officers

The CISA Cybersecurity Advisory Committee shall select a Chair and Vice Chair from among its members through a nomination and formal vote. The Chair and Vice Chair will serve for a two-year term. The CISA Cybersecurity Advisory Committee Chair shall preside at all CISA Cybersecurity Advisory Committee meetings, unless chaired by the Vice Chair, DFO, or ADFO. In the Chair's absence, the Vice Chair will act as the Chair. Additionally, the CISA Cybersecurity Advisory Committee shall select a member to serve as chairperson of each subcommittee.

14. Subcommittees

The Director, through the DFO, establishes subcommittees for any purpose consistent with this charter. The DFO will coordinate with the HSAC DFO to ensure that subcommittees are established in such a manner as to minimize duplication and ensure complementary work activities between both groups.

The CISA Cybersecurity Advisory Committee Chair shall appoint members to subcommittees and shall ensure that each member appointed to a subcommittee has subject matter expertise relevant to the subject matter of the subcommittee. Such subcommittees may not work independently of the chartered committee and must present their advice or work products to the CISA Cybersecurity Advisory Committee for full deliberation and discussion.

Each subcommittee shall meet semiannually, at a minimum, and submit to the CISA Cybersecurity Advisory Committee for inclusion in the annual report, activities, findings, and recommendations, regarding subject matter considered by the subcommittee.

Subcommittees have no authority to make decisions on behalf of the CISA Cybersecurity Advisory Committee and may not report directly to the Federal Government or any other entity.

15. Recordkeeping:

The records of the CISA Cybersecurity Advisory Committee, formally and informally established subcommittees, or other subgroups of the Committee shall be handled in accordance with General Records Schedule 6.2, or other applicable and approved agency records disposition schedule. These records shall be available for public

inspection and copying in accordance with the Freedom of Information Act (Title 5, United States Code, section 552).

16. Filing Date:

May 21, 2021

Department Approval Date

May 24, 2021

GSA Consultation Date

June 25, 2021

Date Filed with Congress

September 3, 2021

Date Amendment Filed with Congress

DEFENDANTS' EXHIBIT 121:



AMERICA'S CYBER DEFENSE AGENCY

SHARE:    

MEETING AGENDAS

CISA Cybersecurity Advisory Committee (CSAC) Meeting Resources

Quarterly meeting agendas and summaries

Publish Date: March 13, 2023





View the quarterly meeting agendas and summaries for each CISA Cybersecurity Advisory Meeting starting from December 2021 to present.


Resource Materials


-  **March 2023 CSAC Quarterly Meeting Agenda** /sites/default/files/2023-03/csac_march-quarterly-meeting_open-session-agenda_2023-03-06_508.pdf
(PDF, 145.04 KB)
-  **March 2023 CSAC Quarterly Meeting Summary** /sites/default/files/2023-04/csac_march-quarterly-meeting_open-session-summary_2023-04-06_508.pdf
(PDF, 373.99 KB)
-  **December 2022 CSAC Quarterly Meeting Agenda** /sites/default/files/2023-02/december_2022_csac_quarterly_meeting_agenda_pdf_192_kb.pdf
(PDF, 192.74 KB)
-  **December 2022 CSAC Quarterly Meeting Summary**
/sites/default/files/publications/csac_december-quarterly-meeting-summary_508_01062023_0.pdf
(PDF, 245.04 KB)
-  **September 2022 CSAC Quarterly Meeting Agenda** /sites/default/files/2023-02/september_2022_csac_quarterly_meeting_agenda_pdf_60_kb.pdf
(PDF, 60.02 KB)

 **September 2022 CSAC Quarterly Meeting Summary** </sites/default/files/2023-02/september_2022_csac_quarterly_meeting_summary_pdf_175_kb.pdf>
(PDF, 175.83 KB)


 **June 2022 CSAC Quarterly Meeting Agenda**
</sites/default/files/publications/june_22_2022_csac_quarterly_meeting_open_agenda-5-27-22_508.pdf>
(PDF, 180.04 KB)

 **June 2022 CSAC Quarterly Meeting Summary**
</sites/default/files/publications/csac_june_quarterly_meeting_summary.pdf>
(PDF, 211.43 KB)

 **March 2022 CSAC Quarterly Meeting Agenda**
</sites/default/files/publications/draft%2520csac%2520march%252031%2520quarterly%2520meeting%2520full%2520agenda%2520%25283-29-2022%2529.pdf>
(PDF, 174.86 KB)

 **March 2022 CSAC Quarterly Meeting Summary**
</sites/default/files/publications/csac%2520quarterly%2520meeting%2520summary_march%2520session%2520%25283-31-22%2529_508.pdf>
(PDF, 242.84 KB)

 **December 2021 CSAC Kickoff Meeting Agenda** </sites/default/files/2023-01/december_2021_csac_kickoff_meeting_agenda_pdf_273_kb.pdf>
(PDF, 273.28 KB)

 **December 2021 CSAC Kickoff Meeting Summary**
</sites/default/files/publications/csac_kickoff_meeting_summary_open_session-508.pdf>
(PDF, 220.26 KB)

Cybersecurity Best Practices </topics/cybersecurity-best-practices>

Organizations and Cyber Safety </topics/cybersecurity-best-practices/organizations-and-cyber-safety>

Cyber Threats and Advisories </topics/cyber-threats-and-advisories>

Related Resources

PUBLICATION

CISA Cybersecurity Advisory Committee (CSAC) Fact Sheet </resources-tools/resources/cisa-cybersecurity-advisory-committee-csac-fact-sheet>

MAR 20, 2023 ■ PUBLICATION

Cybersecurity Advisory Committee (CSAC) Subcommittee Fact Sheet </resources-tools/resources/cybersecurity-advisory-committee-csac-subcommittee-fact-sheet>

MAR 06, 2023 ■ PUBLICATION

2022 Cybersecurity Advisory Committee (CSAC) Reports and Recommendations </resources-tools/resources/2022-cybersecurity-advisory-committee-csac-reports-and-recommendations>

JAN 27, 2023 ■ PUBLICATION

Secure Your Drone: Privacy and Data Protection Guidance </resources-tools/resources/secure-your-drone-privacy-and-data-protection-guidance>

[Return to top](#)

Topics </topics>

Spotlight </spotlight>

Resources & Tools </resources-tools>

News & Events </news-events>

Careers </careers>

About </about>



**CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY**



CISA Central

888-282-0870

Central@cisa.dhs.gov

CISA.gov

An official website of the U.S. Department of Homeland Security

[About CISA </about>](#)

[Accessibility <https://www.dhs.gov/accessibility>](https://www.dhs.gov/accessibility)

[Budget and Performance <https://www.dhs.gov/performance-financial-reports>](https://www.dhs.gov/performance-financial-reports) [DHS.gov <https://www.dhs.gov>](https://www.dhs.gov)

[FOIA Requests <https://www.dhs.gov/foia>](https://www.dhs.gov/foia)

[No FEAR Act </cisa-no-fear-act-reporting>](#)

[Office of Inspector General <https://www.oig.dhs.gov/>](https://www.oig.dhs.gov/)

[Privacy Policy </privacy-policy>](#)

[Subscribe](#)

[The White House <https://www.whitehouse.gov/>](https://www.whitehouse.gov/)

[USA.gov <https://www.usa.gov/>](https://www.usa.gov/)

[Website Feedback </forms/feedback>](#)



**CISA
CYBERSECURITY
ADVISORY
COMMITTEE**

MEETING AGENDA

Tuesday, March 21, 2023

OPEN SESSION

3:15 p.m. – 4:00 p.m. EDT

- 3:15 p.m. Call to Order and Opening Remarks**
- Ms. Megan Tsuyi, Cybersecurity and Infrastructure Security Agency (CISA) Cybersecurity Advisory Committee (CSAC) Designated Federal Officer
 - Mr. Tom Fanning, CSAC Chair
 - Mr. Ron Green, CSAC Vice Chair
 - The Honorable Jen Easterly, Director, CISA
- 3:25 p.m. CSAC Recommendations Discussion**
- Jen Easterly, Director
 - Committee Members
- 3:35 p.m. Subcommittee Updates**
- Jen Easterly, Director
 - Committee Members
- 3:50 p.m. Public Comment Period**
- 4:00 p.m. Closing Remarks**
- Jen Easterly, Director
 - Tom Fanning, Chair
 - Ron Green, Vice Chair



CISA CYBERSECURITY ADVISORY COMMITTEE

CISA CYBERSECURITY ADVISORY COMMITTEE MARCH 21, 2023 MEETING SUMMARY

OPEN SESSION

Call to Order and Opening Remarks

Mr. Tom Fanning, Cybersecurity and Infrastructure Security Agency (CISA) Cybersecurity Advisory Committee (CSAC) Chair, Southern Company, and CSAC Vice Chair, Mr. Ron Green, Mastercard, welcomed participants and the 13 new CSAC members. Mr. Fanning outlined the Committee's focus to build upon the work from the CSAC's inaugural year and provide recommendations related to new scoping documents.

Ms. Megan Tsuyi, CISA, reviewed that the *Federal Advisory Committee Act* governs the CSAC. She reiterated that, while members of the public had the opportunity to provide public comments during the meeting, the Committee did not receive any requests to provide public comment. She informed the public that written comments are accepted at any time.

The Honorable Jen Easterly, Director, CISA, welcomed participants and introduced the new members. She recognized that Mr. Bobby Chesney, UT Austin, had resigned from the Committee and thanked him for his efforts, highlighting his support to Austin's 3-1-1 program. Director Easterly expressed pride in the diverse background of the members and expressed confidence that the Committee is well-positioned to ensure that target-rich, cyber-poor entities are better served and supported.

CSAC Recommendations Discussion

Director Easterly announced that CISA received formal recommendations from the CSAC at the September 2022 Quarterly Meeting and distributed the response to the recommendations to the Committee. She indicated that all recommendations and responses are on the CISA website. CISA accepted or partially accept all 29 recommendations approved by the CSAC.

Director Easterly noted that the resolutions of the CSAC subcommittees were to identify and address key priorities for 2023. She stressed that the essential first step of identifying and managing risk is to identify systemically important entities (SIEs). CISA plans to work carefully with Sector Risk Management Agencies (SRMAs) to identify initial SIEs and develop a program of enhanced engagement with previously identified entities, with an end date goal of September. CISA plans on standing up a SIE program office to help carry out this important work.

Director Easterly explained that CISA was established four years ago to serve as America's cyber defense agency and the national coordinator for critical infrastructure resilience. To ensure robust cyber hygiene, CISA will focus on target-rich, cyber-poor sectors to include K-12 education, healthcare and hospitals, and water and wastewater. Director Easterly explained that these sectors were chosen because they were monitored by other SRMAs but are still building their capacity to confront cyber threats. She explained the importance of building partnerships with each entity.

Director Easterly confirmed that CISA remains committed to sharing information on up-to-date research on current and emerging threats to election officials. CISA will continue to support state and local election officials by providing the most up-to-date information to be used to reduce the risk of foreign influence and election security threats on US election processes.

Mr. Fanning thanked Director Easterly for addressing the CSACs detailed recommendations with such thoughtful responses.

CSAC Subcommittee Updates

Director Easterly led subcommittee chairs in a discussion on top priorities for 2023.

The Building Resilience & Reducing Systemic Risk to Critical Infrastructure Subcommittee is focusing on collaboration to understand interdependencies within the private sector and government. The subcommittee aims to bolster the nation's defense system by guiding CISA's work on SIEs, CISA's development of a national cyber risk register, and how CISA can work with SRMAs. CISA leadership stressed the importance of persistent collaboration and reviewed CISA's actions to create a Joint Collaborative Environment (JCE). The JCE would serve as a unique information-sharing platform for partners across the federal government and industry leaders to conduct analysis to build national security resilience.

The National Cybersecurity Alert System Subcommittee highlighted the success of CISA's Shields Up campaign, with the accepted reality of the nation's inability to put shields down. The subcommittee is leveraging the successes of CISA's Shields Up campaign and the success of other models in the US to create an actionable alert system.

The Transforming the Cyber Workforce Subcommittee is focusing on recommendations to enhance the full spectrum of CISA's talent management ecosystem to build upon and sustain a people-first culture. The subcommittee will provide recommendations on how to effectively utilize CISA's Chief People Officer and (Acting) Chief Human Capital Officer, assess the effectiveness of CISA's hybrid work environment, and address burnout and workload concerns.

The Turning the Corner on Cyber Hygiene Subcommittee will focus heavily on product safety to ensure technology products are both secure-by-design and secure-by-default. The subcommittee will also provide support to target-rich, cyber-poor entities such as K-12 schools, hospitals, and the water and wastewater sector. CSAC members discussed ways CISA could best promote product safety and support target-rich, cyber-poor entities.

The Technical Advisory Council Subcommittee is focusing on memory safety and high-risk community protection. CISA leadership reflected on the need to mature technology products and shift toward a holistic response to advanced persistent threats. CISA leadership referenced the *Foreign Affairs* article authored by Director Easterly and the CISA Executive Assistant Director for Cybersecurity, Mr. Eric Goldstein.¹

The Corporate Cyber Responsibility Subcommittee stressed the need for CISA to better engage with corporate boards to improve national cyber resiliency. CSAC members identified an overlap between the need to better engage both private and public sectors, such as K-12 school districts, to strengthen the nation's cyber defense.

Closing Remarks

Director Easterly offered her gratitude to CSAC for the incorporated, implemented, and impactful work accomplished in the past fiscal year, and the meaningful work and solutions to come.

Mr. Fanning thanked the members of the public and the media in attendance, the support staff, and the CSAC for a successful meeting. He noted that the official CSAC meeting summaries can be found on the CISA website. The CSAC will convene in-person for the next quarterly meeting in June in the Washington D.C. area. Mr. Fanning adjourned the CSAC March 2023 Quarterly Meeting.

¹ <https://www.foreignaffairs.com/authors/jen-easterly>

APPENDIX: OPEN SESSION PARTICIPANT LIST

CSAC Members

Name	Organization
Steve Adler	Former Mayor of Austin, TX
Marene Allison	Former Johnson & Johnson
Lori Beer	JPMorgan Chase
Dave DeWalt	NightDragon
Tom Fanning	Southern Company
Brian Gagnolati	Atlantic Health Systems
Ron Green	Mastercard
Royal Hansen	Google
Niloofar Razi Howe	Tenable
Rahul Jalali	Union Pacific
John Katko	Former U.S. House of Representatives
Jim Langevin	Former U.S. House of Representatives
Doug Levin	K12 Security Information eXchange (K12 SIX)
Kevin Mandia	Mandiant
Ciaran Martin	National Cyber Security Centre
Jeff Moss	DEF CON Communications
Nicole Perloth	Cybersecurity Journalist
Matthew Prince	Cloudflare
Ted Schlein	Kleiner Perkins
Robert Scott	New Hampshire Department of Environment Services
Suzanne Spaulding	Center for Strategic and International Studies
Kevin Tierney	General Motors
Alex Tosheff	VMware
Nicole Wong	NWong Strategies

Government Participants

Name	Organization
The Hon. Jen Easterly	CISA
Alaina Clark	CISA
Victoria Dillon	CISA
Jonathan Dunn	CISA
Lisa Einstein	CISA
Jamie Fleece	CISA
Eric Goldstein	CISA
Kirsten Heidelberg	CISA
Helen Jackson	CISA
Elizabeth Kolmstetter	CISA
Kiersten Todt	CISA
Megan Tsuyi	CISA
Kim Wyman	CISA

Contractor Support

Name	Organization
James Eustice	Edgesource
Mariefred Evans	TekSynap
Lauren Rousseau	Edgesource
Xavier Stewart	Edgesource

Public Participants

Name

Natalie Alms
Karin Athanas
Mariah Bailey
Riley Beggin
Gary Berman
Calvin Biesecker
Ashley Billings
Paul Brandau
Lyn Brown
Aaron Burrows
Sarahjane Call
Carolyn Prill
Thomas Cross
Sunil Dadlani
Brett DeWitt
Anne Disse
Grace Dille
Justin Doubleday
Dennis Dunckel
Ben Flatgard
Matthew Fisch
Sara Friedman
Eric Geller
Jonathan Greg
Michele Guido
Rola Hariri
Simha Himakuntala
Zach Howell
Madeline Hughes
Sara Jacob
Albert Kammler
Matt Kehoe
Norma Krayem
Audrey LaForest
Thomas Leithauser
David Macklin
Megan Mance
Katrina Manson
Hector Guillermo Martinez
Tomas Maldonado
George McElwee
Georgia McLean
Maggie Miller

Organization

FCW
TIC Council Americas
TekSynap
Detroit News
Cyber Heroes Comics
Defense Daily
CNN
CISA
Wiley Rein LLP
Aleta Technologies
DHS/CMO
American Gas Association
Channel Partner.TV
Atlantic Health Systems
Mastercard
Apple
MeriTalk
Federal News Network
American Fair Credit Council
JPMorgan Chase
Eclipses
Inside Cybersecurity
Freelance Journalist
The Record
Southern Company
Department of Defense
Oakridge National Laboratory
Hill East Group
LexisNexis Publication
CISA
Van Scoyoc Associates
Apple
Van Scoyoc Associates
Automotive News
Cybersecurity Policy Report
Homeland Security & Defense Forum
Homeland Security Dialogue Forum
Bloomberg News
GM Sectec
National Football League
Commonwealth Strategic Partners
Wilkinson Barker Knauer, LLP
POLITICO

Avery Mulligan	CISA
Devi Nair	Center for Strategic and International Studies
Brendan Peter	SecurityScorecard
Kevin Piekarski	CISA
Joshua Quaye	Murphy, Pearson, Bradley, & Feeney PC
Shannon Riley	CISA
Mike Rosen	NightDragon
Alec Rosin	CISA
Edison Shen	Security Industry Association
Cedric Sharps	TekSynap
Edison Shen	Security Industry Association (SIA)
Travis Stoller	Wiley Rein LLP
Claire Teitelman	JPMorgan Chase
Timothy Thatcher	USAA
Charles Tupitza	National Cyber Security Center
Christian Vasquez	CyberScoop
Jackie Valley	The Christian Science Monitor
Michael Wayland	CNBC
Angela Weinman	VMware

CERTIFICATION

I hereby certify that, to the best of my knowledge, the foregoing minutes are accurate and complete.

Mr. Tom Fanning (approved on 03 April 2023)
CISA Cybersecurity Advisory Committee Chair



**CISA
CYBERSECURITY
ADVISORY
COMMITTEE**

Apple Park
One Apple Park Way
Cupertino, CA 95014

**MEETING AGENDA
OPEN SESSION**

Tuesday, December 6, 2022
1:00 p.m. – 3:00 p.m. PST

- 1:00 p.m. Call to Order and Opening Remarks**
- Ms. Megan Tsuyi, Cybersecurity and Infrastructure Security Agency (CISA) Cybersecurity Advisory Committee (CSAC) Designated Federal Officer
 - Mr. Tom Fanning, CSAC Chair
 - Mr. Ron Green, CSAC Vice Chair
 - The Honorable Jen Easterly, Director, CISA
- 1:10 p.m. CSAC Recommendations Discussion**
- Jen Easterly, Director
 - Committee members
- 1:30 p.m. Member Roundtable on CSAC Strategic Focus for 2023**
- Jen Easterly, Director
 - Committee members
- 2:45 p.m. CSAC Annual Report Overview**
- Tom Fanning, Chair
- 2:50 p.m. Public Comment Period**
- 3:00 p.m. Closing Remarks and Adjournment**
- Jen Easterly, Director
 - Tom Fanning, Chair
 - Ron Green, Vice Chair



CISA CYBERSECURITY ADVISORY COMMITTEE

CISA CYBERSECURITY ADVISORY COMMITTEE DECEMBER 6, 2022 MEETING SUMMARY

OPEN SESSION

Call to Order and Opening Remarks

Mr. Tom Fanning, CISA Cybersecurity Advisory Committee (CSAC) Chair, Southern Company, reviewed the Committee's accomplishments during its inaugural year. He reflected on the impact of the CSAC's contributions. Mr. Fanning and Mr. Ron Green, Mastercard, thanked the CSAC members and CISA partners for their work.

Ms. Megan Tsuyi, CISA, stated that the *Federal Advisory Committee Act* governs the CSAC. She reviewed that members of the public had the opportunity to provide public comments during the meeting, but the Committee did not receive any requests to provide public comment. She informed the public that written comments are accepted at any time.

The Honorable Jen Easterly, Director, CISA, emphasized the value of the Joint Cyber Defense Collaborative (JCDC) and Shields Up campaign as capabilities of America's Cyber Defense Agency. She acknowledged the CSAC's input is essential for CISA's evolution into the cyber defense agency that the United States needs and deserves.

CSAC Recommendations Discussion

Director Easterly reviewed the CSAC's work advancing the taskings to date to include standing up six subcommittees in December 2021 and adding a seventh subcommittee following the June 2022 Quarterly Meeting. She added that the CSAC and its subcommittees have met 94 times over the course of the year.

To date, CISA has received 48 recommendations from the CSAC which are posted on the CSAC website.¹ Director Easterly reviewed that out of the first 24 recommendations submitted, CISA has fully or partially accepted nearly all of them. CISA has completed at least two recommendations to date, to include the hiring of a Chief People Officer, Dr. Elizabeth Kolmstetter, and holding a "What to Expect on Election Day" workshop with state and local election officials. Director Easterly applauded CSAC members for distilling the taskings to make specific, actionable recommendations.

To refocus CSAC efforts in 2023, Director Easterly discussed the CSAC strategic plan for 2023: (1) Transforming the Cyber Workforce Subcommittee will focus recommendations on CISA's talent management and hiring practices; (2) the Turning the Corner on Cyber Hygiene Subcommittee will focus on shaping the technology ecosystem to be secure by design, providing support to target-rich and cyber-poor entities, and leveraging the cyber performance goals to achieve this work; (3) the Technical Advisory Council Subcommittee will strengthen partnerships with the hacker and research communities and source ideas on how CISA can promote memory safe code to support the work of the Cyber Hygiene Subcommittee; (4) the Building Resilience & Reducing Systemic Risk to Critical Infrastructure Subcommittee will provide guidance on CISA's work on Systemically Important Entities, CISA's development of a National Cyber Risk Register, and how CISA can work with Sector Risk Management Agencies to materially and measurably reduce risk; (5) the National Cybersecurity Alert System Subcommittee will provide ideas for how CISA can calibrate responses to cyber threats based on risk severity to promote sustainable risk management; (6) the Strategic Communications and Protecting Critical Infrastructure from Misinformation & Disinformation Subcommittees will stand down, as they have successfully answered their taskings and provided recommendations to CISA; and (7) the CISA Director will establish a new subcommittee focused on Corporate Cyber

¹ <https://www.cisa.gov/cisa-cybersecurity-advisory-committee-reports-and-recommendations>

Responsibility (CCR) which will work to establish and amplify best practices for technology ecosystems that are secure by design and promote persistent collaboration with partners, focusing on target-rich, cyber-poor entities.

Member Roundtable

Director Easterly confirmed that CSAC Chair, Mr. Fanning, would contact CSAC members to determine subcommittee assignments for the 2023 calendar year.

Committee members discussed the CSAC's newest study addressing the topic of corporate cyber responsibility, and how it can encourage corporate boards to promote strong cyber hygiene. Members agreed that CCR initiatives would better integrate cybersecurity best practices into the fabric of society. Ms. Nicole Wong, NWong Strategies, encouraged CISA to use this as an opportunity to build relationships at the state government level to strengthen the communication channels and relationships between sectors.

Mr. Ted Schlein, Kleiner Perkins, explained the need to define what successful cybersecurity practices look like and encouraged CISA to incentivize companies to achieve that success. Mr. Alex Stamos, Krebs Stamos Group, noted that the traditional role of a board in cybersecurity may be outdated. He suggested that providing guidance on how to proactively address cyber threat to corporate boards and C-suite executives might help them to stay engaged with the mission.

CSAC members discussed the root problems of the current technology ecosystem, such as the fact that two-thirds of vulnerabilities are due to memory unsafety, which is directly tied to programming languages. Members stressed that now is the time for CISA to raise awareness and organizations to raise to act.

Annual Report Overview

Mr. Fanning highlighted the annual report requirement mandated in section 2216 of the *National Defense Authorization Act of 2021*². He presented key points from the CSAC 2022 Annual Report to CISA Director Easterly. CSAC convened during 4 quarterly meetings; CSAC and its subcommittees met 94 times; and CSAC presented 48 recommendations to CISA.

Closing Remarks

Director Easterly reviewed CISA's progress in reviewing and addressing CSAC recommendations. She thanked the Committee for the valuable work done in 2022 and conveyed her excitement for the work that will be completed in 2023.

Mr. Fanning emphasized the ongoing lethal threat to the United States' critical infrastructure and the importance of the CSAC's work. Mr. Fanning and Mr. Green thanked Director Easterly for her leadership and Mr. George Stathakopoulos, Apple, for hosting the meeting. Mr. Fanning adjourned the December CSAC Quarterly Meeting.

² <https://www.congress.gov/bill/116th-congress/house-bill/6395/text>

APPENDIX: OPEN SESSION PARTICIPANT LIST

CSAC Members

Name

Lori Beer
Bobby Chesney
Tom Fanning
Vijaya Gadde
Ron Green
Kevin Mandia*
Jeff Moss*
Nuala O'Connor*
Nicole Perlroth
Mathew Prince
Ted Schlein
Suzanne Spaulding*
Alex Stamos
Kate Starbird
George Stathakopoulos
Alicia Tate-Nadeau*
Nicole Wong

Organization

JPMorgan Chase
University of Texas School of Law, Austin
Southern Company
Former Twitter Chief Legal Officer
Mastercard
Mandiant
DEF CON Communications
Walmart
Cybersecurity Journalist
Cloudflare
Kleiner Perkins
Center for Strategic and International Studies
Krebs Stamos Group
University of Washington
Apple
Illinois Emergency Management Agency
NWong Strategies

Government Participants

Name

The Hon. Jen Easterly
The Hon. Chris Inglis
Alaina Clark
Jonathan Dunn
Lisa Einstein
Maria Gilbert
Eric Goldstein
Mona Harrington
Helen Jackson
Elizabeth Kolmstetter
Bob Lord
Nitin Natarajan
David Rosado
Taylor Smith
Kiersten Todt
Megan Tsuyi

Organization

CISA
Office of the National Cyber Director
CISA
CISA
CISA
CISA
CISA
CISA
CISA
CISA
CISA
CISA
CISA
CISA
CISA

Contractor Support

Name

James Eustice*
Mariefred Evans
Lauren Rousseau
Xavier Stewart

Organization

Edgesource
TekSynap
Edgesource
Edgesource

In-Person Participants

Name

Anne Disse
William Garrity
Katey Harrison
Matt Kehoe
Dan Koslofsky
Jeff Ratner

Organization

Apple
Mastercard
Apple
Apple
Apple
Apple

Name

Jason Sanford
 Candace Laurett Sikora

Organization

Illinois Emergency Management Agency
 Apple

Dialed In Participants*

Name

Mariam Baksh
 Jeff Brancato
 Brett DeWitt
 Sara Friedman
 Eric Geller
 Michele Guido
 Kirsten Heidelberg
 Gwainevere Hess
 Joey Hewitt
 Tom Leithauser
 Sean Lyngaas
 Celinda Moening
 Stacy O'Mara
 Devi Nair
 Jennifer Pedersen
 Lisabeth Perez
 John Sakellariadis
 Nicole Sganga
 Cedric Sharps
 John Shumate
 Travis Stoller
 Christian Vasquez
 Andrea Vittorio
 Erin Wieczorek
 Leah Young

Organization

NextGov
 Northeast Ohio CyberConsortium
 Mastercard
 Inside Cybersecurity
 Politico
 Southern Company
 CISA
 CISA
 Plains All American Pipeline
 Telecommunications Reports
 CNN
 CISA
 Mandiant
 Center for Strategic and International Studies
 CISA
 MeriTalk
 Politico
 CBS News
 CISA
 Apple
 Wiley Rein LLP
 Cyberscoop
 Bloomberg Industry Group
 CISA
 CISA

*Denotes an individual who participated virtually. Note: all dialed in participants attended virtually.

CERTIFICATION

I hereby certify that, to the best of my knowledge, the foregoing minutes are accurate and complete.

Mr. Tom Fanning (approved on 05 January 2023)
CISA Cybersecurity Advisory Committee Chair



CISA CYBERSECURITY ADVISORY COMMITTEE

MEMBER MEETING AGENDA

Tuesday, September 13, 2022

OPEN SESSION

2:00 p.m.

Call to Order and Opening Remarks

- Megan Tsuyi, Cybersecurity and Infrastructure Security Agency (CISA) Cybersecurity Advisory Committee (CSAC) Designated Federal Officer
- Jen Easterly, Director, CISA
- Tom Fanning, CSAC Chair
- Ron Green, CSAC Vice Chair

2:10 p.m.

Public Comment Period

2:25 p.m.

Subcommittee Updates/Deliberation and Vote

- Tom Fanning, Building Resilience and Reducing Systemic Risk to Critical Infrastructure, and Establishment of a National Cybersecurity Alert System
- Kate Starbird, Protecting Critical Infrastructure from Misinformation and Disinformation
- George Stathakopoulos, Turning the Corner on Cyber Hygiene
- Ron Green, Transforming the Cyber Workforce
- Jeff Moss, Technical Advisory Council
- Niloo Howe, Strategic Communications

3:55 p.m.

Closing Remarks and Adjournment

- Jen Easterly, Director
- Tom Fanning, Chair
- Ron Green, Vice Chair



CISA CYBERSECURITY ADVISORY COMMITTEE

CISA CYBERSECURITY ADVISORY COMMITTEE SEPTEMBER 13, 2022, MEETING SUMMARY

OPEN SESSION

Call to Order and Welcoming Remarks

Ms. Megan Tsuyi, Cybersecurity and Infrastructure Security Agency (CISA) Cybersecurity Advisory Committee (CSAC) Designated Federal Officer, called the meeting to order. She reviewed the *Federal Advisory Committee Act* rules governing the meeting and noted that while the Committee advertised the opportunity for public comment there had been no requests from the public to provide comment.

The Hon. Jen Easterly, CISA Director, welcomed the attendees and briefly reviewed the background and intent of the CSAC. The Director announced the completion and distribution of CISA's Strategic Plan for 2023 - 2025. She then asked Mr. Brandon Wales, Executive Director, CISA, to introduce the four pillars of the plan.

Operational Updates

Mr. Wales provided a high-level overview of the CISA Strategic Plan. He reflected on the overall mission focusing on the resiliency and security of the Nation's critical infrastructure. He highlighted the four pillars approach of the CISA Strategic Plan: 1) spearhead efforts to make a more resilient cyberspace; 2) determine how to reduce risks and strengthen the Nation's critical infrastructure; 3) ensure close operational coordination and information sharing; and 4) determine how to make CISA a more effective and efficient organization. Mr. Wales reiterated that the CISA Strategic Plan is a starting point for CISA moving forward over the next three years.

Director Easterly described CISA's effort to align Agency goals and objectives with specific measurements that help reduce risk. She pointed out that the Strategic Plan highlights many of the undertakings CISA accomplished since its establishment, including the launch of the Shields Up campaign. Director Easterly then asked Mr. Eric Goldstein, Executive Assistant Director for Cybersecurity, CISA, to provide an operational update.

Mr. Goldstein stated that CISA remains vigilant against threats, even though the Nation has not suffered a major cyber-attack. He cited the recent major cyber intrusions across the globe, including the recent attack in the Albanian government, Great Britain, and the prevalence of ransomware attacks across the globe. He provided an overview of CISA objectives, including promoting steps entities may take to bolster their own security and readiness. He emphasized the recent cross-sector discussion to share information to establish best mitigation practices to secure networks independently.

Mr. Goldstein announced the launch of the Joint Ransomware Task Force, established by Congress and co-chaired by CISA and the Federal Bureau of Investigation (FBI), and its goal to reduce the impact of ransomware by cross-sector collaboration to determine best practices of tackling the emergent threat of ransomware intrusion. He continued with a review of CISA's Cybersecurity Awareness Month.

Director Easterly introduced Mr. Tom Fanning, CSAC Chair, Southern Company to provide opening remarks and lead the discussion through the seven Subcommittee updates.

Mr. Fanning welcomed CSAC Members and expressed his gratitude for their work on the CSAC. He emphasized the importance of CSAC's recommendations to the Nation's future, and significant value produced by the discussions surrounding these issues. He clarified the schedule of the session and opened the floor for opening comments to Mr. Ron Green, CSAC Vice Chair, Mastercard.

Mr. Green reflected that CSAC has made tremendous strides over the past year collaborating between the public and private sector. He shared his enthusiasm for CSAC's continued achievements and recommendations to bolster the efficiency and resiliency of the Nation's cybersecurity.

Subcommittee Updates

Building Resilience and Reducing Systemic Risk to Critical Infrastructure

Mr. Fanning thanked the Building Resilience and Reducing Systemic Risk to Critical Infrastructure (SR) Subcommittee members and credited the individuals who contributed to the SR Subcommittee's report to the CISA Director.

Mr. Fanning summarized the three pillars in the SR report: 1) the "who" pillar identifies systemically important entities (SIEs); 2) the "what" pillar specifies resiliency goals for orderly and efficient action; and 3) the "how" pillar details programs and structures that enable resiliency goals. He reviewed key findings from the SR Subcommittee's research, including the significant disparity in maturity levels of SIEs, the importance of shared national goals, the need to avoid economic calamity, and the value in harmonizing cyber regulations. He encouraged CISA to consider replacing Executive Order 13636 Improving Critical Infrastructure Cybersecurity Section 9 entities with the SIEs.

Mr. Fanning reviewed the SR recommendations within each pillar:

1. Identify SIEs. Collaborate with the private sector on shared obligations. Engage SIEs to identify risk derivatives, coordinate cross-sector risks, and prioritize responses to emerging risks based on impact. Prepare SIEs for triage capabilities.
2. Develop a common framework with shared language and goals. Create a culture that unifies CISA, sector risk management agencies, the intelligence community, the private sector, and other national stakeholders.
3. Establish goals. Construct an analytic framework with baseline risk management. Provide a forum for business partners to identify their assets and practices. Build an integrated approach to resilience and a maturity model that evaluates performance. Address the perspectives of system owners and operators in addition to their Chief Executive Officers and Chief Information Security Officers. Leverage existing regulations and avoid duplication. Focus on outcomes rather than processes. Demonstrate the value of participation.

Ms. Lori Beer, JPMorgan Chase, thanked the SR Subcommittee's subject matter experts. She expounded on the value of collaboration within the financial industry. She recognized the government's ability to provide unique capabilities to the private sector.

Ms. Marene Allison, Johnson & Johnson, explained that some industries have already organized themselves, and others would benefit from the frameworks (e.g., Information Sharing and Analysis Centers [ISACs]) that deliver national insights).

Mr. Kevin Mandia, Mandiant, advocated for a test, respond, remediate, and repeat cycle to identify deficiencies and improve the work product. He emphasized the importance of testing and operationalizing recommendations within the third "how" pillar.

Mr. Fanning informed the group that the SR Subcommittee conducted two tabletop exercises during its information gathering stage.

Mr. Green remarked that transparent goals would incentivize companies to correct their own issues before a regulator prompts the company to take corrective actions. Mr. Fanning agreed with the comment, and he mentioned that transparency is iterative.

Mr. Ted Schlein, Kleiner Perkins, thanked the SR Subcommittee members for their work. He asked about the message to entities that pay taxes and want access to the government even though they are not SIEs. Mr. Fanning responded that the SIE designation enables asset prioritization, real-time evaluation of the cyber battlefield, consistent responses, and valuable feedback loops to share the SIEs' lessons learned with other entities via the

ISACs. He acknowledged that there may be timing differences (e.g., declassification of information), but he concluded that everyone would benefit from these recommendations.

Ms. Nicole Wong, NWong Strategies, asked if the Transforming the Cyber Workforce (TCW) and SR Subcommittees should work together to address talent gaps. Mr. Fanning encouraged collaboration between all CSAC Members.

Director Easterly applauded the SR Subcommittee's comprehensive work on the report and recommendations. She underscored the importance of their work for CISA's core mission and its ongoing efforts to collaborate, reduce risk, measure outcomes. Director Easterly described several no-cost services that CISA publishes for non-SIEs. She acknowledged the usefulness of the SIE designation in responding to and recovering from major cybersecurity incidents.

CSAC Members voted on and unanimously approved the recommendations.

Protecting Critical Infrastructure from Misinformation and Disinformation

Ms. Suzanne Spaulding, Center for Strategic and International Studies, thanked **Protecting Critical Infrastructure from Misinformation and Disinformation (MDM)** Subcommittee Chair Dr. Kate Starbird, University of Washington, for her leadership and reviewed that she would lead the Subcommittee's update in Dr. Starbird's absence.

Ms. Spaulding briefly summarized the Subcommittee's focus on addressing the urgent risk facing U.S. elections and election officials. She upheld that elections have a critical national function to faithfully reflect the will of the people and secure a peaceful transition of power.

Ms. Spaulding reviewed that the recommendations emphasize the need for CISA to focus on threats to U.S. elections and election officials. Such threats manifest in two ways: 1) cyber-enabled threats designed to reduce public trust in the legitimacy of the elections process; and 2) broader mis- and dis-information operations the public continues to see. The recommendations aim to help CISA better support state and local election officials dealing with both types of threats. She reviewed the key findings from the MDM Subcommittee's work to ensure CISA coordinates directly with the Intelligence Community (IC), including the FBI, to prioritize the needs of election officials and identify intelligence requirements at a local level. Subcommittee members suggest CISA contact election officials to identify current needs. She noted that the recommendations are affirmed by state and local election officials themselves.

Ms. Spaulding reviewed the second set of recommendations that advise CISA to help the courts ensure the resolution of disputes and the peaceful transfer of power, as the courts have become a significant target of mis- and dis-information attacks. The Subcommittee expanded on the earlier set of recommendations presented during the CSAC June Quarterly Meeting. The Subcommittee emphasized CISA's role to provide resources, best practices, templates, and website guidance to state and local election officials to give them the tools needed to proactively address mis- and dis-information. The Subcommittee suggested CISA leverage its far-reaching platform by amplifying state and local resources on its communications channels. Ms. Spaulding stressed that elections must be managed at the local level by local election officials, but upheld CISA's role to provide needed resources. Regarding threats from foreign adversaries, the report recommended that CISA promptly share information from the IC with state and local election officials.

Director Easterly thanked the Subcommittee for their work and stressed that CISA is committed to remaining non-partisan and non-political as the Agency works with every state and local election official to address the concern of how mis- and dis-information impacts election operations. She reaffirmed CISA's commitment to upholding civil rights and civil liberties that are at the core of the American democracy. She reviewed CISA's actions to date in this space to include the CISA Joint Cyber Defense Collaborative (JCDC)'s toolkit of free election security resources tailored to election officials. She further emphasized that CISA's role is not to run elections, but to share resources with election officials. She detailed CISA's focus to empower election officials to manage threats through coordinated vulnerability discovery and disclosure support, working with state vendors on disclosure programs, providing physical security including insider threat guidance, and releasing associated trainings online for rapid

access. Director Easterly commended the Subcommittee for their focus on supporting work with the courts.

Mr. Schlein suggested CISA remove the wording of mis- and dis-information due to its politicization. He recommended framing discussions around CISA's work providing the American people with accurate information.

CSAC Members voted on and unanimously approved the recommendations.

Turning the Corner on Cyber Hygiene

Mr. George Stathakopoulos, Apple, identified the **Turning the Corner on Cyber Hygiene** (CH) Subcommittee's focus and security requirements. Mr. Stathakopoulos noted that the Subcommittee centered their original efforts on targeting small and medium organizations, places that cannot provide their own IT security and cyber hygiene. This idea has since expanded to include the entire spectrum of organizations.

Mr. Stathakopoulos reviewed the CH Subcommittee's previous recommendation for CISA to focus on Multi-Factor Authentication (MFA). He encouraged CISA to saturate the cybersecurity landscape with this message as much as possible and partner with large companies to amplify this message. He suggested that large companies could also pledge their support to encourage other organizations to enable MFA. He detailed the Subcommittee's earlier recommendation for CISA to support and expand upon the Austin 311 pilot program which has been tested already.

Mr. Bobby Chesney, University of Texas, described the current partnership University of Texas, Austin, and the City of Austin has with various private sector entities. He campaigned for the need to scale up the required talent to enact a national partnership and solicit inquiries on how that might be possible. He submitted that the goal was pioneering a direct intersection between various cities and CISA, to establish partnerships. Mr. Stathakopoulos added that CISA should use metrics gathered through the partnership in Austin, Texas to determine emergent CISA partnerships.

Mr. Stathakopoulos opened the floor to comments and questions from the attendees. Ms. Marene Allison, Johnson & Johnson, noted that it might be more effective to focus messaging senior corporate (C-Suite) executives and resiliency forums, as opposed to only Chief Security Officers. Ms. Nuala O'Connor, Walmart, responded that the recommendations are pointed toward all C-Suite executives. Mr. Green added that it would be beneficial to push these recommendations to boards of directors as well. Director Easterly clarified the importance of a robust cyber ecosystem to all boards of directors, as cyber security is business security.

Mr. Stathakopoulos added that the next step would be to find new potential targets and centralize partnerships.

Director Easterly stressed that cyber risk is business risk is national risk. She also expressed support for the idea of a cyber hotline.

Transforming the Cyber Workforce

Mr. Green thanked the **Transforming the Cyber Workforce** (TCW) Subcommittee members and reviewed the TCW Subcommittee's ongoing assessment of curricula, candidate qualifications, and service requirements for people who participate in the government's cybersecurity programs. He discussed efforts to attract cybersecurity talent, to identify pipelines that match talent with opportunities at CISA, to research cyber skills, and to evaluate the availability of apprenticeships and mentorships. Mr. Green addressed upcoming efforts to study the decentralized workforce and propose recommendations at the CSAC December Quarterly Meeting.

Mr. Chris Young, Microsoft, commented on the relationship between the TCW Subcommittee's work and other CSAC Subcommittee's initiatives. He identified the cyber skillset as a common denominator, and he noted the potential for collaboration.

Director Easterly announced that CISA's new Chief People Officer (CPO) will join in October 2022. She asserted that the CPO would help to unify these efforts. Ms. Kiersten Todt, Chief of Staff, CISA, summarized an initiative between the Department of Commerce, Department of Labor, the National Institute of Standards and Technology, and CISA to promote cyber apprenticeships and job retraining. Mr. Green indicated that the TCW Subcommittee would include that initiative in its research.

Strategic Communications

Ms. Niloofer Razi Howe, Tenable, thanked the **Strategic Communications (SC)** Subcommittee members. Ms. Howe commended CISA on their various outreach and newly released Strategic Plan that imparts unity of effort, unity of message, and practical details that support cybersecurity practitioners.

Ms. Howe reviewed the SC Subcommittee's contributions to several CISA initiatives, including the CISA.gov website redesign. Ms. Howe elaborated that the website must reflect the mission and goals of CISA, starting with a complete redesign. She addressed CISA's unique challenge to serve myriad stakeholders with a broad range of perspectives. She affirmed the SC Subcommittee's support for future iterations of the website. Ms. Howe also offered the SC Subcommittee's support for any approved CSAC recommendations.

Ms. Nicole Perlroth, Cybersecurity Journalist, added that the SC Subcommittee sees itself as a partner to the other CSAC Subcommittees and that it is prepared to support in any way possible.

Technical Advisory Council

Mr. Eric Goldstein, CISA, briefed on the **Technical Advisory Council (TAC)** Subcommittee's efforts in the absence of Subcommittee Chair Mr. Jeff Moss, DEF CON Communications. He affirmed the Subcommittee's support of the recommendations accepted by the full Committee during the CSAC June Quarterly Meeting regarding vulnerability discovery and disclosure and cyber threat intelligence sharing. He reviewed the Subcommittee's actions to date to include meeting with stakeholders across critical infrastructure and state, local, territorial, and tribal governments for additional context on how CISA interacts with key partners and to inform the group's next set of recommendations. He thanked the Subcommittee members for their work reviewing CISA's guidance to small businesses and reviewing challenges in reaching critical threat areas.

Director Easterly affirmed the significant level of support the TAC Subcommittee members have given CISA by providing feedback on ways to engage small businesses.

Closing Remarks and Adjournment

Director Easterly thanked the CSAC Members for their attendance and contribution to the discussion. She announced that the next CSAC Quarterly Meeting will be on December 6, 2022.

Director Easterly informed the Committee that CISA is working through the recommendations from the CSAC June Quarterly Meeting. She stated that CISA will finalize its response by October 6, 2022. She elaborated that the response will explain how the Agency plans to implement the recommendations, and that it will be consistent with the CISA Strategic Plan released on September 13, 2022. Director Easterly also introduced Ms. Lisa Einstein, CSAC Executive Director, CISA, and stated that her role would be to help bolster the CSAC's work.

Mr. Fanning thanked everyone for their recommendations and commitment to refining the work that the CSAC has produced. He acknowledged the Committee's role in producing meaningful results and improving cybersecurity outcomes for the U.S. He encouraged each member to be aspirational in their thinking, and he conveyed his excitement and appreciation for the CSAC's work.

Mr. Fanning adjourned the September Quarterly Meeting.

APPENDIX: CLOSED SESSION PARTICIPANT LIST

CSAC Members

Marene Allison
 Lori Beer
 Bobby Chesney
 Tom Fanning
 Ron Green
 Niloofar Razi Howe
 Kevin Mandia
 Jeff Moss
 Nuala O'Connor
 Nicole Perlroth
 Ted Schlein
 Steve Schmidt
 Suzanne Spaulding
 Alex Stamos
 George Stathakopoulos
 Nicole Wong
 Chris Young

Organization

Johnson & Johnson
 JPMorgan Chase
 University of Texas School of Law, Austin
 Southern Company
 Mastercard
 Tenable
 Mandiant
 DEF CON Communications
 Walmart
 Cybersecurity Journalist
 Kleiner Perkins
 Amazon
 Center for Strategic and International Studies
 Krebs Stamos Group
 Apple
 NWong Partners
 Microsoft

Government Participants

Director Easterly
 Alaina Clark
 Victoria Dillon
 Lisa Einstein
 Trent Frazier
 Eric Goldstein
 Mona Harrington
 Nitin Natarajan
 Jen Pedersen
 Kiersten Todt
 Megan Tsuyi
 Brandon Wales
 Kim Wyman

Organization

CISA
 CISA
 CISA
 CISA
 CISA
 CISA
 CISA
 CISA
 CISA
 CISA
 CISA
 CISA

CSAC Support

Mariah Bailey
 Jonathan Dunn
 Lisa Einstein
 James Eustice
 Mariefred Evans
 Sonja Grant
 Nayeema Hoq
 Celinda Moening
 Lauren Rousseau
 Barry Skidmore
 Xavier Stewart

Organization

Edgesource
 CISA
 CISA
 Edgesource
 TekSynap
 CISA
 CISA
 CISA
 Edgesource
 CISA
 Edgesource

Other Attendees

Karin Athana
 Mariam Baksh
 Robert Barton
 Ashley Billings
 Pascal Boctor
 Ian Brown
 AmyClaire Brusch
 Ross Clark
 Anne Disse
 Justin Doubleday
 Adrienne Dowling
 Mathew Eggers
 Kelly Feili
 Ben Flatgard
 Amy Flowers
 Bree Fowler
 Benjamin Freed
 Sara Friedman
 Will Garrity
 Elizabeth Gauthier
 Eric Geller
 Kegan Gerard
 Mardy Goote
 Aileen Graef
 Jonathan Greig
 Michele Guido
 Judith Harroun-Lord
 Gabe Hengel
 Gwainevere Hess
 Joey Hewitt
 Nicole Hodziewich
 Kathryn Ignaszewski
 Abi Kinnard
 Norma Krayem
 Navid Kreshavarz-Nia
 Danouh Louis
 Jerry Markon
 Alexandra Martin
 Scott McConnell
 Jennifer McGrath
 Devi Nair
 Stacy O'Mara
 Theresa Paraschac
 Jacob Phillips
 Dylan Presman
 Katheryn Rosen
 Geneva Sands
 Robert Schill
 Cedric Sharps
 Jordana Siegel
 Samuel Spector
 Claire Teitelman

Organization

TIC Council Americas
 Government Executive Media Group
 Plains All American Pipeline, L.P.
 CNN
 Cornerstone Government Affairs
 CISA
 Airports Council International – North America
 CISA
 Apple
 Federal News Network
 CISA
 US Chamber of Commerce
 Depository Trust and Clearing Corporation
 JPMorgan Chase
 Microsoft
 CNET
 StateScoop/EdScoop
 Inside Cybersecurity
 Mastercard
 CISA
 Politico
 Southern California Edison
 Software & Information Industry Association
 CNN
 The Record
 Southern Company
 Transportation Security Administration
 CISA
 CISA
 Plains All American Pipeline
 Lockheed Martin
 IBM
 Cornerstone Government Affairs
 Van Scoyoc Associates
 Raytheon Technologies Corporation, Raytheon Intelligence & Space
 CISA
 MeriTalk
 CISA
 CISA
 Unum Law
 Center for Strategic and International Studies
 Mandiant
 Depository Trust and Clearing Corporation
 MISO
 Office of the National Cyber Director
 JPMorgan Chase
 CNN
 Blackberry
 TekSynap
 Amazon
 Blackberry
 JPMorgan Chase

Other Attendees (Cont.)

Erik Thomas
Liz Turrell
Christian Vasquez
Keith Woolford

Organization

Systems Engineering
CNN
E&E News
Siemens DIS

CERTIFICATION

I hereby certify that, to the best of my knowledge, the foregoing minutes are accurate and complete.

Tom Fanning (approved on 12 October 2022)

Mr. Tom Fanning
CISA Cybersecurity Advisory Committee Chair
October 12, 2022



**CISA
CYBERSECURITY
ADVISORY
COMMITTEE**

Austin Central Library
Special Event Center
710 W. Cesar Chavez St.
Austin, TX 78701

MEMBER MEETING AGENDA

Wednesday, June 22, 2022
12:00 p.m. – 2:30 p.m. CT

- 12:00 p.m. Call to Order and Opening Remarks**
- Ms. Megan Tsuyi, Cybersecurity and Infrastructure Security Agency (CISA) Cybersecurity Advisory Committee (CSAC) Designated Federal Officer
 - The Honorable Jen Easterly, Director, CISA
 - Mr. Tom Fanning, CSAC Chair
 - Mr. Ron Green, CSAC Vice Chair
- 12:15 p.m. Public Comment Period**
- 12:30 p.m. Subcommittee Updates/Deliberation and Vote**
- Ron Green, Transforming the Cyber Workforce
 - George Stathakopoulos, Turning the Corner on Cyber Hygiene
 - Jeff Moss, Technical Advisory Council
 - Kate Starbird, Protecting Critical Infrastructure from Misinformation and Disinformation
 - Tom Fanning, Building Resilience and Reducing Systemic Risk to Critical Infrastructure
 - Niloo Howe, Strategic Communications
- 2:30 p.m. Closing Remarks and Adjournment**
- Jen Easterly, Director
 - Tom Fanning, Chair
 - Ron Green, Vice Chair



CISA CYBERSECURITY ADVISORY COMMITTEE

CISA CYBERSECURITY ADVISORY COMMITTEE June 22, 2022, MEETING SUMMARY

OPEN SESSION

Call to Order and Welcoming Remarks

Ms. Megan Tsuyi, Cybersecurity and Infrastructure Security Agency (CISA) Cybersecurity Advisory Committee (CSAC) Designated Federal Officer, called the meeting to order. She reviewed the *Federal Advisory Committee Act* rules governing the meeting and noted that there were no requests for public comment.

Director Jen Easterly, CISA, welcomed the attendees and thanked Mayor Steve Adler, Austin, Texas, and Mr. Bobby Chesney, Dean Designate, University of Texas Austin Law School, for hosting the CSAC June Quarterly Meeting. Director Easterly updated the committee on actions CISA has taken since the CSAC Kickoff Meeting in December 2021 to include mitigating the risk of the Log4Shell vulnerability, CISA's actions in response to Russia's invasion of Ukraine, strengthening the Shields Up campaign, and the Joint Cyber Defense Collaborative (JCDC). Director Easterly expressed gratitude to members for their advice and counsel to respond to the initial taskings with thoughtful and creative recommendations. Director Easterly outlined the path forward in responding to the recommendations within 90 days and emphasized her full commitment to transparently sharing how CISA would implement those recommendations.

She reviewed the CSAC's new tasking focused on the feasibility of an alert system for cyber risk to ensure the nation is not operating at a Shields Up, highest posture of alert, at every moment. She reviewed the cyber advisory threat alert system tasking which will target businesses large and small and offer very specific, actionable steps.

Director Easterly applauded the work of the subcommittees to date and welcomed Mr. Tom Fanning, CSAC Chair, Southern Company, to provide opening remarks.

Mr. Fanning welcomed CSAC Members and expressed his gratitude to members for their work on the CSAC. He emphasized that not only are the CSAC's recommendations themselves important to the country's future, but the discussions surrounding these issues will produce a significant value.

Mr. Ron Green, CSAC Vice Chair, Mastercard, reflected that the recommendations were a direct result of the CSAC's commitment to the cybersecurity mission. He commented that he was encouraged by what the members were able to accomplish and what each subcommittee continues to do.

Mr. Fanning confirmed with Ms. Tsuyi that there is a public comment period, but there are no public comments to discuss. He outlined the agenda for the afternoon session to designate approximately 20 minutes of discussion per subcommittee to include updates and any items for full CSAC vote. Mr. Fanning turned the meeting over to Mr. Green for his updates on the Transforming the Cyber Workforce Subcommittee.

Subcommittee Updates

Transforming the Cyber Workforce

Mr. Green emphasized the Transforming the Cyber Workforce Subcommittee's commitment to their work. The subcommittee's recommendations were broken down into two categories: CISA's workforce challenges and national challenges.

In addressing CISA's workforce challenges the CSAC recommends that CISA prioritize strategic workforce development, dramatically improve its talent acquisition process to be competitive with the private sector, radically expand recruitment efforts to identify candidates across their professional lifecycle, and leverage talent identification and hiring success through interagency collaboration. He commended CISA for taking the initial steps to hire a Chief People Officer.

He noted that CISA must dramatically improve hiring goals and processes and recommended that CISA lower the hiring timeframe to 90 days to delivery of a Temporary Job Offer (TJO). He reviewed the suggestion for CISA to develop a systemic approach to collecting and analyzing data on candidate pools and hiring processes, review hiring goals with senior leadership, and move to more flexible and manageable results.

Mr. Green stressed that closing the agency's talent gap will require rapidly expanding recruitment efforts. Current recruiting pools do not encompass the entire spectrum of talent. To improve hiring practices, CISA should establish a standard working group to advise on best practices, utilize guidance from public and private sector advisors, and expand internship opportunities to recruit emerging talent. He encouraged CISA to conduct these actions through a thorough review of the interagency security clearance process and develop a senior leader specific hiring strategy. Director Easterly asked Mr. Green to have the subcommittee review the Agency's security clearance process to determine ways to better streamline it.

Mr. Green emphasized the need for creative, new programs which would lower the barrier of access into cyber security positions. He noted the recent establishment of CISA's Cyber Innovation Fellows as one great example. The committee suggests that CISA open a cyber academy which will partner with the private sector and community colleges and universities along with other industry supported cyber education providers, develop a cyber security training curriculum which will be taught at academic institutions, and unify the cyber oriented programs under one junior cyber corps umbrella.

The committee recommended CISA establish a cyber force program and a peace corps like cyber program. This program would provide education and service to provide domestic security development assistance.

Director Easterly thanked the subcommittee for their ambitious and actionable recommendations. She commended the subcommittee for providing actionable recommendations.

CSAC Members unanimously approved the recommendations.

Turning the Corner on Cyber Hygiene

Mr. George Stathakopoulos, Apple, identified the **Turning the Corner on Cyber Hygiene** Subcommittee's focus and security requirements. He shared the recommendation that CISA build out its current multi-factor authentication (MFA) campaign by identifying additional vehicles for publicizing "More Than a Password", take all available steps to ensure that companies working with the federal government fully adopt MFA by 2025, and that CISA launch a "311 National" campaign that provides an emergency call line and clinics for assistance with cyber incidents for small and medium businesses. He encouraged CISA to make the recommendations clear and attractive and make it easier for companies to receive the help they need.

Mr. Chesney recommended that CISA partner with cities and universities to complete the "311 National" line. Mr. Stathakopoulos noted that the recommendations are the initial steps in a long journey towards securing the American public and businesses. He stressed the need for over-saturation in that CISA should amplify cyber hygiene messaging across all audiences and communications forums.

Mr. Eric Goldstein, CISA, added that accessing talent pools within cities and universities might allow CISA to deploy talent, such as computer science and engineering students or law and business students, to work for credits or pro bono in clinics.

CSAC Members provided feedback on the recommendations. Mr. Green commended the subcommittee on the simplicity of their approach to the MFA campaign by helping the average person. Mr. Fanning stated that he is

encouraged by the subcommittee's systemic thinking.

Director Easterly expressed her excitement for "More Than a Password" and noted that they launched the campaign at the RSA Conference in the beginning of June. She also thanked the subcommittee for their idea of a local partnership and Mayor Adler for volunteering to use Austin as a pilot.

CSAC Members unanimously approved the recommendations.

Technical Advisory Council

Mr. Jeff Moss, DEF CON Communications, reviewed the composition of the **Technical Advisory Council (TAC)** Subcommittee and detailed the two recommendations on coordinated vulnerability discovery and disclosure (CVD) and cyber threat intelligence (CTI).

Mr. Moss explained the CVD recommendations are externally focused and detailed the difficulties in reporting vulnerabilities. He stressed that CISA, as the nation's cyber defense agency, can make the reporting process more attractive. He noted that the researcher community has limited time and energy to report vulnerabilities and the more complicated the process, the less likely they will report a detected vulnerability. He encouraged CISA to develop incentives and access to information to aid security researchers who will submit vulnerabilities affecting critical systems. CISA should work to enable a frustration-free CVD process by working with Congress and sector-specific regulatory agencies to require that manufacturers supply firmware images of every released version for the industry, which should ultimately be archived for future automated analysis. He urged CISA to invest in a central platform to facilitate the intake of suspected vulnerabilities and communication between security researchers, agencies, and vendors. While the Vulnerability Information and Coordination Environment (VINCE) is not the prescribed solution, Mr. Moss recommended that CISA adapt a system similar to VINCE. Mr. Moss recommended that CISA simplify the reporting process and provide feedback to those reporting.

Mr. Moss reviewed the second, internally facing recommendation on CTI and shared the impression that CISA is doing well in this area, but the recommendations feature overall observations on areas of improvement. He recommended that CISA automate this process to start with the users most in need. He recommended that CISA invest in a program to make CTI available to all qualified users and eliminate barriers to access such as high costs. This would significantly benefit smaller organizations in need of additional CTI assistance. CISA should also invest in enriching CTI reports to increase durability across all layers of defense. He also encouraged CISA to explore techniques to enable scalable and effective development of expertise in CTI.

Mr. Goldstein noted the recommendations would be extraordinarily impactful in enhancing CISA's ability to act as a trusted broker of the CVD process to work collaboratively with vendors to reduce the risk of exposure.

Mr. Fanning asked Mr. Moss to clarify how he envisioned a frustration-free reporting process. Mr. Moss reflected on a briefing from the Food and Drug Administration to note the wide range in complexities throughout each sector's reporting process. He stressed that CISA can provide value by vetting information to determine who the vulnerability affects so it is clearly communicated and alleviates the work of the researcher.

Ms. Nicole Wong, NWong Strategies, suggested that CISA consider posing these recommendations to the Cyber Innovation Fellows program Director Easterly is establishing. Mr. Chris Young, Microsoft, underscored the importance of CISA's role in the CVD process to bridge the wide gap in complexities between sectors and organizations.

CSAC Members unanimously approved the recommendations.

Protecting Critical Infrastructure from Misinformation and Disinformation

Dr. Kate Starbird, University of Washington, highlighted the difficulty of the **Protecting Critical Infrastructure from Misinformation and Disinformation Subcommittee's** tasking in today's complex environment. She recommended that CISA take the same action in response to countering mis-, dis-, and mal-information (MDM) as the Agency does to counter cyber threats. She defined the scope of the recommendations in the elections context and

emphasized the expressed need from elections officials from all political parties to do this work, given the acute struggle of elections officials—especially those in small jurisdictions—to address and understand MDM threats. She noted that MDM threats undermining trust in the elections process has led to physical threats against elections officials, reaching the highest level of death threats and attempts to enact harm. Dr. Starbird recommended that CISA focus on informing the public on MDM threats and partner with frontline elections officials to inform the public and point to first-hand elections resources from Secretaries of State. She emphasized that CISA should not prescribe any messaging, but rather point to resources from the state-level.

Dr. Starbird reviewed the four MDM recommendations to CISA. She encouraged CISA to follow a resilience-based approach to launch a broad public awareness campaign on MDM to enhance individual and collective resilience. The campaign should include civics education to understand how to identify MDM and build an understanding of why citizens should not want to spread MDM. She noted that this aligns with CISA's cyber hygiene mission. Dr. Starbird encouraged CISA to proactively address anticipated MDM threats through education. This response should be in the form of pointing to trusted and authoritative sources of information at the local level—in particular, local election officials. She encouraged CISA to rapidly respond to emerging threats in a transparent manner. Dr. Starbird suggested that CISA identify, communicate, and respond to actor-based threats.

She encouraged CISA to support local elections officials by convening a “What to expect on election day” workshop to provide a platform for elections officials themselves to share best practices. She noted the subcommittee's path forward to continue to work through the more challenging questions.

Ms. Alicia Tate-Nadeau, Illinois Emergency Management Agency, emphasized the expressed need from elections officials for guidance on how to counter MDM threats. She stressed that the recommendations are focused on providing tools to elections officials so that they themselves can develop their own best practices.

Ms. Suzanne Spaulding, Center for Strategic and International Studies, reinforced Dr. Starbird's points and thanked her for her leadership. She recognized that public trust is essential in this work and stressed the urgent need to support state and local elections officials.

Director Easterly noted that CISA is beholden to supporting and defending the Constitution and helping to safeguard free and fair elections as the Sector Risk Management Agency for election infrastructure security is part of that mission. She underscored that the federal government's role is not to run elections, but to provide support and resources to every state and locality to help them ensure the security and resilience of elections. Dr. Starbird highlighted Ms. Kim Wyman's, CISA, participation in the subcommittee as a former Republican Secretary of State. Dr. Starbird shared a quote from Mr. Steven Richer, Maricopa County Recorder, Georgia, that “responding to misinformation is my day job. My night job is running elections.”. She stressed that the subcommittee's work is focused on supporting elections officials from all parties across the country. Director Easterly again stressed the criticality of transparency and maintaining trust with the American people.

Mr. Fanning commended Dr. Starbird on her work.

CSAC Members unanimously approved the recommendations.

Building Resilience & Reducing Systemic Risk to Critical Infrastructure

Mr. Fanning reviewed the **Building Resilience & Reducing Systemic Risk to Critical Infrastructure** Subcommittee's actions to examine CISA's work on the concept of Systemically Important Entities (SIE) and the Agency's efforts to enhance resilience across the nation's 55 National Critical Functions (NCFs). He explained that the subcommittee developed two tabletop exercises (TTXs) simulating cyberattacks on the generate electricity NCF to inform their recommendations that will be made to CISA during the CSAC September Quarterly Meeting. He detailed the goal of the TTXs is to break down risk to identify interdependencies and gaps to target systemic risk.

Mr. Fanning stated that the subcommittee will now focus on collaboration responses and how to integrate with the JCDC, the Federal Emergency Management Agency, and State, and Local governments.

Mr. Kevin Mandia, Mandiant, added that the TTXs will help CISA iron out communication issues before a threat arrives.

Director Easterly noted the evaluation of risk on critical infrastructure is a core mission of CISA. She thanked the subcommittee and expressed her excitement to receive their recommendations in September.

Strategic Communications

Ms. Niloofar Razi Howe, Tenable, reviewed the goal of the **Strategic Communications** Subcommittee to enhance CISA's strategic communications efforts, outreach, and partnerships. She reflected on the subcommittee's success partnering with other CSAC Subcommittees to improve their effectiveness and help drive outcomes.

Two of the recommendations were in support of the Turning the Corner on Cyber Hygiene Subcommittee to include the More Than A Password campaign and the Austin 311 Pilot. Regarding the "More Than A Password" campaign, Ms. Howe encouraged CISA to designate a program manager to work with Fortune 500 companies to define their commitment to providing resources, establishing metrics to drive success, and develop a full campaign around cyber hygiene. Regarding the Austin 311 Pilot, Ms. Howe encouraged CISA to create a playbook to identify the process to enable a nationwide program rollout with as little friction as possible.

Ms. Howe recommended that CISA build a broader base of support. She applauded CISA for building trust and support with partners and stakeholders and encouraged CISA to build upon this strength by bringing in cyber reporters for regular briefings. She highlighted the importance of expanding CISA's list of Agency validators to secure allies and amplifiers before CISA news is released. This is an opportunity to build trust and confidence in the U.S. Government's work more broadly.

Director Easterly affirmed the importance of the subcommittee's work, as many members of the public are unaware of CISA's core mission. She thanked the subcommittee for partnering with other efforts and for recruiting cybersecurity journalists. She flagged that the CISA Cybersecurity Awareness Month is approaching in October and this will present additional opportunities for the subcommittee.

CSAC Members unanimously approved the recommendations.

Closing Remarks and Adjournment

Mr. Fanning thanked CSAC Members for their diligence and thoughtfulness in crafting the recommendations. Director Easterly restated her gratitude to the members for developing specific, actionable recommendations.

Mr. Fanning reminded public participants that a meeting summary will be available on the CSAC website and reminded members that the next CSAC Quarterly Meeting is scheduled for September 13, 2022. Mr. Fanning adjourned the meeting.

APPENDIX: OPEN SESSION PARTICIPANT LIST

CSAC Members

Mr. Steve Adler

Ms. Marene Allison

Mr. Robert Chesney

Mr. Thomas Fanning

Ms. Vijaya Gadde

Mr. Ron Green

Ms. Niloofar Razi Howe

Mr. Kevin Mandia

Mr. Jeff Moss

Ms. Nicole Perlroth

Mr. Matthew Prince

Ms. Suzanne Spaulding

Dr. Kate Starbird

Mr. George Stathakopoulos

Ms. Alicia Tate-Nadeau

Ms. Nicole Wong

Mr. Chris Young

Organization

City of Austin, Texas

Johnson & Johnson

University of Texas

Southern Company

Twitter

Mastercard

Tenable

Mandiant

DEF CON Communications

Cybersecurity Journalist

Cloudflare

Center for Strategic and International Studies

University of Washington

Apple

Illinois Emergency Management Agency

NWong Strategies

Microsoft

Government Participants

The Hon. Jen Easterly

Ms. Alaina Clark

Ms. Victoria Dillon

Ms. Stephanie Doherty

Mr. Jonathan Dunn

Mr. Eric Goldstein

Ms. Mona Harrington

Mr. Bob Lord

Ms. Celinda Moening

Mr. Johnathan Moor

Ms. Jennifer Pederson

Mr. Harvey "PT" Perriott

Mr. Kris Rose

Mr. Rob Russell

Mr. Taylor Smith

Ms. Kiersten Todt

Ms. Megan Tsuyi

Ms. Kim Wyman

Organization

CISA

CISA

CISA

CISA

CISA

CISA

CISA

CISA

CISA

CISA

CISA

CISA

CISA

CISA

CISA

CISA

CISA

CISA

Contractor Support

Ms. Mariefred Evans
 Ms. Marissa Pope
 Ms. Thais Price
 Mr. Xavier Stewart

Organization

TekSynap
 EdgeSource
 TekSynap
 EdgeSource

In-Person Participants

Mr. Brett DeWitt
 Ms. Anne Disse
 Mr. Benjamin Flatgard
 Ms. Michele Guido
 Mr. Gary Luedecke
 Ms. Devi Nair
 Ms. Stacy O'Mara
 Ms. Jordana Siegel

Organization

Mastercard
 Apple
 JPMorgan Chase
 Southern Company
 City of Austin, Texas
 Center for Strategic and International Studies
 Mandiant
 Amazon Web Services

Dial-In Participants

Ms. Mariah Bailey
 Ms. Mariam Baksh
 Mr. Calvin Biesecker
 Mr. Scott Bouboulis
 Ms. Dana Bostian
 Mr. Evan Burke
 Ms. Emily Burns
 Ms. Cynthia Brumfield
 Mr. Jack Cable
 Ms. Sarahjane Call
 Mr. Chris Cook
 Mr. Joseph Chilbert
 Mr. Cameron Dixon
 Mr. Justin Doubleday
 Mr. Luiz Eduardo
 Mr. Matt Eggers
 Ms. Lisa Einstein
 Mr. Michael Feldman
 Mr. Matthew Fleisher-Black
 Ms. Amy Flowers
 Mr. David Forsey
 Ms. Sara Friedman
 Mr. Matthew Gasser

Organization

TekSynap
 Nextgov
 Defense Daily
 Wiley Rein LLP
 Bostian Captioning
 U.S. House of Representatives
 U.S. House of Representatives
 Metacurty
 HSGAC
 DHS
 Appropriations - U.S. Senate
 Office of Partnership Engagement
 CISA
 Federal News Network
 Aruba Threat Labs
 U.S. Chamber of Commerce
 Federation of American Scientists
 CISA
 The Cybersecurity Law Report
 Microsoft
 CISA
 Inside Cybersecurity
 TSA

Dial-In Participants (Cont.)

Ms. Elizabeth Gauthier
Mr. Eric Geller
Ms. Aileen Graef
Ms. Sonja Grant
Ms. Carmen Hadgraft
Ms. Gwen Hess
Mr. Edward Humphrey
Mr. Zachary Isakowitz
Mr. Adam Israelevitz
Mr. Alexander Jacobs
Mr. David Jones
Mr. Albert Kammler
Mr. Matt Kehoe
Ms. Norma Krayem
Ms. Christina Lee
Mr. Tom Leithauser
Ms. Oumou Ly
Mr. Joseph Marks
Mr. Martin Matishak
Ms. Neysa Matthews
Mr. Glenn Merell
Mr. Mike Miron
Mr. Phu Nguyen
Mr. Andrew Nicholson
Mr. Jeff Rothblum
Ms. Sophia Salome
Mr. Jason Sanford
Mr. Aaron Schaffer
Mr. Robert Sheldon
Ms. Jenny Shore
Mr. Tim Starks
Mr. Travis Stoller
Ms. Claire Teitelman
Mr. Christian Vasquez
Mr. Shaun Waterman
Ms. Leah Young

Organization

CISA
Politico
CNN
CBP
Southern Company
CISA
CISA
U.S. House of Representatives
U.S. House of Representatives
DHS
Cybersecurity Dive
Van Scoyoc Associates
Apple
Van Scoyoc Associates
Beacon Global Strategies
Telecommunications Reports and Cybersecurity Policy Report
CISA
Washington Post
The Record
Walmart
Freelance Consulting
DHS
Integrated Cybersecurity Engine
Imperium Global Advisors
U.S. Senate
CISA
Illinois Emergency Management Agency
Washington Post
CrowdStrike
CISA
CyberScoop
Wiley Rein LLP
JPMorgan Chase
E&E News
Waterman Reports
CISA

CERTIFICATION

I hereby certify that, to the best of my knowledge, the foregoing minutes are accurate and complete.

Tom Fanning (approved on 21 July 2022)

Mr. Tom Fanning
CISA Cybersecurity Advisory Committee Chair



CISA CYBERSECURITY ADVISORY COMMITTEE

Member Meeting

Thursday, March 31, 2022
2:00 p.m. – 4:00 p.m. ET

2:00 p.m.

Welcoming Remarks

- The Honorable Jen Easterly, Director, Cybersecurity and Infrastructure Security Agency (CISA)
- Mr. Tom Fanning, CISA Cybersecurity Advisory Committee (CSAC) Chair
- Mr. Ron Green, CISA CSAC Vice Chair

2:10 p.m.

Subcommittee Updates

- Mr. Ron Green, Transforming the Cyber Workforce
- Mr. George Stathakopoulos, Turning the Corner on Cyber Hygiene
- Mr. Jeff Moss, Technical Advisory Council
- Dr. Kate Starbird, Protecting Critical Infrastructure from Misinformation and Disinformation
- Mr. Tom Fanning, Building Resilience and Reducing Systemic Risk to Critical Infrastructure
- Ms. Niloo Howe, Strategic Communications

3:40 p.m.

Public Comment Period

3:50 p.m.

Closing Remarks and Adjournment

- Director Easterly
- Mr. Fanning
- Mr. Green



CISA CYBERSECURITY ADVISORY COMMITTEE

CISA CYBERSECURITY ADVISORY COMMITTEE MARCH 31, 2022, MEETING SUMMARY

OPEN SESSION

Call to Order and Welcoming Remarks

Ms. Megan Tsuyi, Cybersecurity and Infrastructure Security Agency (CISA) Cybersecurity Advisory Committee (CSAC) Designated Federal Officer, called the meeting to order. She provided a short summary of *Federal Advisory Committee Act* rules governing the meeting and then turned the meeting over to CISA Director Jen Easterly.

Director Easterly welcomed the attendees and introduced the Committee's Chair, Mr. Tom Fanning, Southern Company, and Vice Chair, Mr. Ron Green, Mastercard. Director Easterly updated the Committee on actions CISA has taken since the CSAC Kickoff Meeting in December 2021 to include mitigating the risk of the Log4Shell vulnerability, preparing for potential cyber threats emerging from Russia's unjust invasion of Ukraine, launching CISA's Shields Up campaign, and promoting a message of preparation, not panic, in the face of potential cyber-attacks on our critical infrastructure. Director Easterly highlighted the cyber incident reporting legislation and omnibus budget passed to increase CISA's overall funding. Director Easterly reiterated her gratitude for the Committee's feedback and counsel during this challenging operational environment.

Director Easterly commented on CISA's efforts to build trusted and collaborative partnerships with industry and highlighted the importance of the Joint Cyber Defense Collaborative (JCDC)'s work and her intent to scale this model to include more partners and broader collaboration to maximize the benefits to the cybersecurity community. Director Easterly then mentioned the ongoing debate about the need for more regulation in critical infrastructure. She offered her recognition for the value of implementing minimum standards for cybersecurity, but also noted concerns about overly burdensome and unharmonized regulations which can result in compliance box-checking rather than real operational risk reduction. Director Easterly stated the goal of the cyber incident reporting is to add value, not burden, and to make CISA a better partner to industry by increasing transparency and information sharing in a way that prevents future attacks while also protecting the privacy and anonymity of the victim.

Director Easterly applauded the work of the subcommittees to date and welcomed Mr. Fanning to provide opening remarks. Mr. Fanning and Mr. Green thanked Director Easterly and Committee members for their participation and noted the criticality of the subcommittee's work to strengthen our nation's cybersecurity resilience.

Subcommittee Updates

Transforming the Cyber Workforce

Mr. Green emphasized the subcommittee's focus on closing the cyber talent gap for CISA and the Nation. He reviewed the subcommittee's work on helping CISA to develop a human capital strategy, talent pipelines, and retention programs to advance prospective individuals into the cyber industry.

Mr. Green outlined the subcommittee's progress thus far to include conversations with CISA leadership, employees who have gone through the hiring process, hiring managers within CISA, individuals responsible for successful hiring initiatives within the government sector, and other outside organizations that have an interest in helping the nation advance its cybersecurity pipeline. Through these discussions, the subcommittee will consider recommending that CISA shorten the interview process that can take up to six months and implement a sustainable education grant program to develop unrealized talent in underserved communities. Mr. Green stressed that the connective tissue between operational teams at CISA and the private industry needs to be strengthened.

CSAC members discussed the importance of collaboration between public and private sectors to strengthen CISA's hiring efforts. Mr. Fanning noted the difference between attracting employees versus retaining them. In terms of industry and government collaboration, Mr. Green shared the idea of Intergovernmental Personnel Appointments (IPA) to allow the agency to bring individuals from the private sector to serve in a governmental capacity. Mr. Fanning noted that at least 85 percent of the critical infrastructure industry is privately owned, making collaboration necessary to CISA's success. Mr. Ted Schlein, Kleiner Perkins Caufield & Byers, recommended introducing a rapid response team for cyber where CISA can pull together a group of experts quickly to solve a particular problem, then send recommendations back to industry quickly, in comparison to what was described as the IPA program. Mr. Green noted that this idea is not something the subcommittee has explored yet, but it is something they will discuss.

Director Easterly noted the recent deployment of the Cyber Talent Management System (CTMS) which has allowed for more flexibility in reducing the steps to onboarding. Director Easterly recommended that the subcommittee receive a full update on CTMS and provide their feedback to determine if this resolves onerous onboarding issues.

Turning the Corner on Cyber Hygiene

Mr. George Stathakopoulos, Apple, identified the subcommittee's focus as finding a way to simplify security recommendations to small and medium businesses. This aligns with the subcommittee's path forward to execute a holistic, scaled approach to ensure that all organizations have the information and resources needed to implement essential security practices. Due to the limited security resources of small businesses, Mr. Stathakopoulos specified small businesses as the most vulnerable to a potential attack, which could have larger implications across an entire sector. Mr. Stathakopoulos detailed six basic steps for businesses to implement to include: (1) hold trainings; (2) implement multi-factor authentication (MFA); (3) patch known vulnerabilities; (4) enable logging on current system; (5) build an incident response plan; and (6) strengthen cyber resilience. He identified a goal for the subcommittee to impart an amplified message of "More Than A Password" to promote MFA implementation. Mr. Stathakopoulos described the path forward to build coalitions and present these recommendations to Fortune 500 companies, non-profits, and universities. Mr. Stathakopoulos added the subcommittee's second goal is to examine the possibility of an emergency call line for ransomware attacks.

CSAC members discussed ways to strengthen the effectiveness of the outlined recommendations. Members proposed potential incentives for businesses that implement these security strategies ranging from the tax incentives recommended by Mr. Schlein to eliminating the existing "MFA tax," as suggested by Mr. Alex Stamos, Krebs Stamos Group. Mayor Steve Adler, City of Austin, identified areas of collaboration with the Strategic Communications Subcommittee to strengthen the broad messaging efforts. Ms. Nuala O'Connor, Walmart, concurred that this is a joint communications and education effort for small and medium businesses and agreed with the focus on simplifying the security message. Mr. Chris Young, Microsoft, asked the subcommittee to consider small businesses operating on a non-cloud infrastructure and the security issues associated with non-cloud operating platforms.

Technical Advisory Council

Previously known as the Igniting the Hacker Community, Mr. Moss, DEF CON Communications, stated the Technical Advisory Council subcommittee is focused on a broader community than just hackers to further catalyze CISA's relationship with the technical community to shift the balance in favor of network defenders. He identified CISA's difficulty interacting at the individual level and called out the community's lack of trust in organizations and true trust in people. Mr. Moss encouraged CISA to build and maintain trust with the researcher community at a person-to-person level. He stated the subcommittee's efforts to determine the best ways for CISA to ignite the power of the technical community from all backgrounds and experiences to create a trusted partnership with the government and CISA. Mr. Moss detailed the subcommittee's path forward to incentivize and reduce barriers to vulnerability reporting and outlined a range of initiatives on expanding collaboration with the technical community, including hackers, academics, and researchers. Such ideas included easing the reporting process and building web portals for individuals to report incidents online. Finally, he identified the subcommittee's immediate interest in determining what specific problems CISA is aiming to solve.

Committee members offered examples of best practices within their fields and posed questions to Mr. Moss on potential areas for the Technical Advisory Council to consider. Ms. Suzanne Spaulding, Center for Strategic & International Studies, inquired if the subcommittee had discussed the role of transparency in terms of building trust with the government to openly communicate how the government is using the insights shared by this community. Ms. Spaulding expressed a concern of over-classification by the government as a barrier to reporting. Mr. Moss said the subcommittee is also considering the role of the Civil Liberties and Privacy Community in such an effort and agreed with Mr. Fanning and Mr. Schlein on the importance of transparency in building trust. Ms. Marene Allison, Johnson & Johnson, provided an example of incident reporting best practices in the healthcare sector.

Mr. Eric Goldstein, Head of CISA Cyber, outlined another goal of the subcommittee as to understand this community's perceptions about working with government to understand and remove any deterring factors. He added that CISA's goal is also to unpack incentive models around reporting vulnerabilities to CISA in order to drive more effective and regular disclosure. In thinking about incident reporting accountability among CEOs as part of the business control environment, Director Easterly and Mr. Fanning asked the subcommittee to consider developing a guide for board directors on questions they should be asking about cyber security reporting.

Protecting Critical Infrastructure from Misinformation and Disinformation

Dr. Kate Starbird, University of Washington, discussed the subcommittee's actions to date and path forward to confront mis-, dis-, and malinformation (MDM) harmful to critical infrastructure. Dr. Starbird noted the subcommittee is focused on using strategies to prevent MDM during elections to provide a blueprint on targeting MDM in other contexts, and continues to question how CISA can best support the MDM mission. By focusing on elections, Dr. Starbird stated that the subcommittee can examine CISA's mission across four main areas to include: (1) civics and media literacy—enhancing societal resilience to MDM; (2) proactive work of narrative-specific staging of resources and pre-bunking; (3) response through monitoring, identifying, and addressing specific MDM threats; and (4) detect and respond to foreign influence operations. Dr. Starbird outlined the subcommittee's path forward of determining how CISA can participate effectively in election truth narratives and how CISA can build trust within this adversarial space.

Committee members highlighted the focus of MDM as undermining the overall trust in government. Mr. Green offered the recommendation that CISA target already trusted communities within the adversarial space to increase CISA's credibility. Ms. Niloo Razi Howe, Energy Impact Partners, concurred that pre-bunking MDM before it spreads is imperative in this context. She added that increasing transparency and rapidly declassifying information are ways CISA can build alliances to deter bad actors. Committee members noted that operational collaboration is a significant way to combat MDM. Ms. Howe offered to connect the subcommittee to resources outside the academic community working on pre-bunking resources.

Building Resilience & Reducing Systemic Risk to Critical Infrastructure

Mr. Fanning shared that the subcommittee is determining how to best drive national risk management and identify the criteria for scalable, analytic models to prioritize risk. He addressed one of the group's challenges as understanding the bridge between the National Risk Management Center (NRMC) and how to incorporate this work into the JCDC. He noted that the subcommittee is reimagining the notion of national security, focusing on collaborations between the private sector and government to ensure they are not thinking of critical risk sectors in a silo. Mr. Fanning applauded the NRMC for their work examining the national critical functions (NCFs) and the interdependencies among sectors to ensure a sound response to a major incident. He stated that the subcommittee is focused on determining the highest priority NCFs and evaluating realistic scenarios at the asset level. Mr. Fanning shared that the subcommittee is determining recommendations that could be potentially operationalized into policy and law, and how to best define CISA's charge for protecting our critical infrastructure. Mr. Fanning mapped out the subcommittee's path forward to examine specific NCFs including (1) generate electricity, particularly examining risks to pipelines; (2) water; (3) financial services; and (4) telecommunications to then develop scenarios which will explore the impacts at the asset and supply chain levels to determine the corresponding effects of an attack and how collaboration between industry and government can best secure America. Following the scenarios, the subcommittee

will develop a playbook on how to communicate this collaboration.

CSAC members discussed CISA's role in sector risk management without recreating cybersecurity capabilities extensively within other governing departments and agencies. Director Easterly commented that CISA is not looking to replace Information Sharing Analysis Centers (ISACs), but is rethinking ways to share relevant data. Mr. Goldstein commented that sector risk management agencies (SRMAs) provide expertise in sector-specific risks and an understanding of how to expand function resilience within sectors under all conditions. In cyber intrusions, CISA is able to provide generalized cyber expertise which can be applied, combined with the sector-specific knowledge of the SRMAs to drive down risk across sectors at scale. Mr. Goldstein shared that the JCDC is focused on how to generalize and scale the current risk models to increase operational collaboration across sectors as novel risks are identified. This will lead to a force multiplier effect to drive down risk far more quickly than companies can accomplish individually.

Chris Inglis, National Cyber Director, provided an overview of the Office of the National Cyber Director's (NCD) mission to assess the performance of cyber investments including the roles and responsibilities, not just financial investments. He shared that the NCD is currently performing a study in partnership with CISA on the SRMAs to determine recommendations for further action to get each of them up to the level of performing tabletop exercises.

Ms. Allison concluded the subcommittee's updates by highlighting that interconnectivity breeds actionable intelligence and stressed the need to strengthen the partnership between government and industry.

Strategic Communications

Ms. Howe reviewed the subcommittee's task of addressing how CISA can communicate their mission in a way that engages stakeholders around risk management issues. She stated the subcommittee's second focus of exploring how CISA can improve communications to ensure all audiences are informed of CISA's mission and value add to the nation's cyber defenses. She outlined the path forward and current challenges of the subcommittee to include how to be most effective in communicating CISA's mission.

Ms. Howe suggested the subcommittee reconvene to build partnerships between each subcommittee. Ms. Howe identified two action items for the subcommittee, to include (1) identifying the next step as receiving a brief on CISA's longer term strategic communications strategy and (2) receive a brief from each subcommittee chair to determine how the subcommittee can support, develop, and boost communication needs of the Committee as a whole.

Committee members discussed ways to more clearly identify the subcommittee's messaging efforts regarding CISA's mission and value add. Ms. Nicole Perlroth, Cybersecurity Journalist, suggested to conceptualize CISA's messaging in two ways, (1) thinking of the CISA brand itself and (2) how to educate others regarding cyber hygiene. Director Easterly emphasized the importance of CISA being responsive to all feedback and how that directly correlates with the public trusting the Federal Government.

Mr. Fanning thanked the participants for their comments and turned the meeting over to Ms. Tsuyi for the Public Comment Period.

Public Comment Period

Mr. Joe Weiss, Applied Control Solutions, LLC, provided the following comment for the record:

Thank you for this opportunity to provide comment. My comments I think will cover a number of the working groups and it's dealing with engineering considerations. Process sensors and operational technology (OT) networks are used in every physical infrastructure, everything you've been talking about. Securing OT networks is necessary but not sufficient. Compromising the process sensors can damage any process, yet neither the sensor comprised nor the system damaged may be identifiable by the OT networks.

March 10, I gave a university seminar on the lack of cyber security in process sensors titled: "Shields Up and Good Cyber Hygiene Do Not Apply to Insecure Process Sensors". Process sensors have no inherent

cybersecurity but yet have direct connections to the Internet and 100 percent trusted input to OT networks. The cybersecurity gap includes no capability for passwords, single-factor (much less multi-factor) authentication, encryption, keys, signed certificates, etc. Moreover, process sensors have no cyber forensics.

Shields Up recommends conducting a test of manual controls to ensure that critical functions remain operable if the organization's network is unavailable or untrusted. Good cyber hygiene requires strong passwords. However, insecure process sensors have no passwords and are untrusted during all conditions. There have been more than 11 million control systems cyber incidents, many of them process sensor related, directly resulting in more than 1,500 deaths. The vast majority were not identified as being cyber-related, as there are no control systems cyber forensics at the process sensor layer. There's effectively no cybersecurity training for the control and safety systems engineers and technicians—even though cybersecurity training is available for the OT network personnel. Adversaries such as Russia, China, and Iran are aware of these deficiencies. It is not possible to be cyber secure, resilient, or safe if you cannot trust your process measurements.

There are a number of paths for moving forward. In the short term, get the engineers involved. I've heard nothing about that. Use sensor monitoring and analytics at the physics, not end word packet layer, to improve cybersecurity process safety product quality, resilience, and regulatory compliance. That cannot be done by monitoring the OT networks alone. Develop process sensor cyber forensics. Develop training recommendations and standards for process sensors. And in the long term, develop new cyber secure process sensors.

And with that, I really want to appreciate the ability to be able to provide these comments. Thank you.

Mr. Fanning thanked Mr. Weiss. Director Easterly asked Mr. Goldstein to weigh in on Mr. Weiss' remarks. Mr. Goldstein affirmed that industrial control systems (ICS) and OT security are foundational to CISA's mission and remains one of the Agency's top priorities. He stated that CISA needs to benefit from the extraordinary expertise in the research community, vendors, and asset operators to provide the best possible guidance and insights. He shared the example that the vulnerability and disclosure team released over 500 advisories last year on vulnerabilities in ICS and OT devices, each of which were the product of coordination between researchers, vendors, and owner-operators who deploy mitigations. Mr. Goldstein confirmed that CISA does work in collaboration with the engineers who develop the technologies deployed by CISA across ICS systems across the country. He also stressed CISA's goal to build and strengthen partnerships to address today's risks and threats and drive towards a future that is more secure and resilient by design, and process sensors are part of that equation. Mr. Goldstein closed by stating that ICS and OT security is one of CISA's top focus, CISA is working towards strengthening partners with experts across sectors to build a more secure technology ecosystem where control systems are more secure by design.

Closing Remarks and Adjournment

Director Easterly thanked the Committee members and other meeting participants for their subcommittee work and their input during the meeting. She identified trust and collaboration as key themes of the meeting and encouraged the subcommittees to work together to craft recommendations for CISA to share during the June CSAC Quarterly Meeting. Mr. Fanning and Mr. Green both provided brief closing remarks noting that the Committee's work matters and thanked members for their participation. Director Easterly adjourned the meeting.

APPENDIX: OPEN SESSION PARTICIPANT LIST

CSAC Members

Mr. Steve Adler
 Ms. Marene Allison
 Ms. Lori Beer
 Mr. Robert Chesney
 Mr. Thomas Fanning
 Ms. Vijaya Gadde
 Dr. Patrick Gallagher
 Mr. Ron Green
 Ms. Niloofar Razi Howe
 Mr. Kevin Mandia
 Mr. Jeff Moss
 Ms. Nuala O'Connor
 Ms. Nicole Perlroth
 Mr. Ted Schlein
 Mr. Stephen Schmidt
 Ms. Suzanne Spaulding
 Mr. Alex Stamos
 Dr. Kate Starbird
 Mr. George Stathakopoulos
 Ms. Alicia Tate-Nadeau
 Ms. Nicole Wong
 Mr. Chris Young

Organization

City of Austin, Texas
 Johnson & Johnson
 JPMorgan Chase
 University of Texas
 Southern Company
 Twitter
 University of Pittsburgh
 Mastercard
 Tenable
 Mandiant
 DEF CON Communications
 Walmart
 Cybersecurity Journalist
 Kleiner Perkins Caufield & Byers
 Amazon Web Services
 Center for Strategic and International Studies
 Krebs Stamos Group
 University of Washington
 Apple
 Illinois Emergency Management Agency
 NWong Strategies
 Microsoft

Government Participants

The Hon. Jen Easterly
 The Hon. Chris Inglis
 Mr. Robert Costello
 Ms. Alaina Clark
 Mr. Chris DeRusha
 Mr. Jonathan Dunn
 Mr. Trent Frazier
 Mr. Eric Goldstein
 Ms. Mona Harrington
 Ms. Rachel Liang
 Mr. John (Jack) MacNeil
 Ms. Celinda Moening
 Mr. Nitin Natarajan
 Mr. Barry Skidmore
 Ms. Kiersten Todt
 Ms. Megan Tsuyi

Organization

CISA
 NCD
 CISA
 CISA
 Office of Management and Budget
 CISA
 CISA
 CISA
 CISA
 CISA
 CISA
 CISA
 CISA
 CISA
 CISA
 CISA

Ms. Kim Wyman

CISA

Contractor Support

Mr. Joseph Butler

Ms. Mariefred Evans

Ms. Marissa Pope

Organization

TekSynap

TekSynap

EdgeSource

Dial-In Participants

Ms. Mariam Baksh

Mr. Mitchell Berger

Mr. Christopher Bidwell

Mr. Calvin Bieserker

Ms. AmyClaire Brusch

Mr. Jack Cable

Ms. Sarahjane Call

Mr. Dan Callahan

Ms. Anne Cutler

Ms. Jen DeBerge

Mr. Brett DeWitt

Ms. Victoria Dillon

Ms. Osasu Dorsey

Ms. Lisa Einstein

Mr. Benjamin Flatgard

Ms. Amy Flowers

Mr. Christopher Frascella

Ms. Sarah Friedman

Mr. Will Garrity

Ms. Elizabeth Gauthier

Mr. Eric Geller

Ms. Michele Guido

Mr. Geoffrey Hale

Ms. Gwainever Hess

Mr. Edward Humphrey

Ms. Helen Jackson

Mr. Matt Kehoe

Ms. Christina Lee

Mr. Tom Leithauser

Ms. Oumou Ly

Ms. Neysa Matthews

Mr. Glenn Merell

Mr. Mike Miron

Ms. Devi Nair

Mr. Phu Nguyen

Organization

NextGov

Department of Health and Human Services

Airports Council International

Defense Daily

Airports Council International

Senate HSGAC

Department of Homeland Security

Fortinet Federal

CISA

Mastercard

Mastercard

CISA

Office of the National Cyber Director

Stanford

JPMorgan Chase

Microsoft

Electronic Privacy Information Center

Inside Cybersecurity

Mastercard

CISA

POLITICO

Southern Company

CISA

CISA

CISA

CISA

Apple

Beacon Global Strategies

Telecommunications Reports and Cybersecurity Policy Report

CISA

Walmart

Freelance Consulting

Department of Homeland Security

International Security Program

Integrated Cybersecurity Engine

Mr. Andrew Nicholson

Imperium Global Advisors

Dial-In Participants

Ms. Maggie O'Connell
Ms. Stacy O'Mara
Mr. Nick Ornstein
Mr. Marty Reynolds
Mr. Alexander Rodriguez
Ms. Katheryn Rosen
Mr. Jason Sanford
Ms. Jordana Siegel
Mr. Jordan Sims
Mr. Tim Starks
Mr. Travis Stoller
Ms. Claire Teitelman
Mr. Wesley Trimble
Ms. Liz Turrell
Mr. Christian Vasquez
Ms. Nicky Vogt
Mr. Joe Weiss
Ms. Erin Wieczorek
Mr. Ford Winslow

Organization

Interstate Natural Gas Association for America
Mandiant
TwinLogic Strategies
Airlines for America
DP DHL Americas
JPMorgan Chase
Illinois Emergency Management Agency
Amazon
Imperium Global Advisors
CyberScoop
Wiley Law
JPMorgan Chase
Commonwealth Strategic Partners
CNN
E&E News
CISA
Applied Control Solutions, LLC
CISA
Integrated Cybersecurity Engine

CERTIFICATION

I hereby certify that, to the best of my knowledge, the foregoing minutes are accurate and complete.

Tom Fanning (approved on 13 April 2022)

Mr. Tom Fanning
CISA Cybersecurity Advisory Committee Chair



CISA CYBERSECURITY ADVISORY COMMITTEE

MITRE 1 Building
7525 Colshire Drive
McLean, VA 22102

ADMINISTRATIVE SESSION

MITRE 1 Building, Room 1H300

- 9:00 a.m. **Welcoming Remarks**
- The Honorable Jen Easterly, Director, Cybersecurity and Infrastructure Security Agency (CISA)
- 9:15 a.m. **Administrative Brief**
- Federal Advisory Committee Act Overview: Alaina Clark, Assistant Director for Stakeholder Engagement
- 9:30 a.m. **Internal Committee Activity**
- Swearing-in of Committee members
 - Committee Chair and Vice Chair nominations and voting

CLOSED SESSION

MITRE 1 Building, Room TBP

- 10:30 a.m. **Threat Briefing and Discussion**
- Mr. Christopher Porter, National Intelligence Officer for Cyber, Office of the Director of National Intelligence
 - Mr. Rob Joyce, Director of Cybersecurity, National Security Agency
 - Director Easterly
 - Committee members

- 12:00 p.m. **Lunch**

OPEN SESSION

MITRE 1 Building, Room 1H300

- 1:00 p.m. **Call to Order and Opening Remarks**
- Ms. Megan Tsuyi, CISA Cybersecurity Advisory Committee Designated Federal Officer
 - Director Easterly
 - Committee Chair
 - Committee Vice Chair
- 1:10 p.m. **Keynote Address**
- The Honorable John Tien, Deputy Secretary of Homeland Security
- 1:20 p.m. **Fortifying the Nation's Cybersecurity Posture**
- The Honorable Chris Inglis, National Cyber Director
- 1:30 p.m. **CISA Overview**
- CISA Overview: Director Easterly
 - Cybersecurity Division Mission Brief: Mr. Eric Goldstein, Executive Assistant Director for Cybersecurity
 - Systemic Risk & National Critical Functions: Mr. Robert Kolasky, Assistant Director, National Risk Management Center
 - Cyber Talent Management System: Mr. Nitin Natarajan, Deputy Director
- 2:20 p.m. **CISA's Big Challenges & Issue Tasking**
- Director Easterly
 - Committee members
- 3:10 p.m. **Public Comment Period**
- 3:20 p.m. **Closing Remarks and Adjournment**
- Director Easterly
 - Committee Chair
 - Committee Vice Chair



CISA CYBERSECURITY ADVISORY COMMITTEE

CISA CYBERSECURITY ADVISORY COMMITTEE DECEMBER 10, 2021, MEETING SUMMARY

OPEN SESSION

Call to Order and Opening Remarks

Ms. Megan Tsuyi, Cybersecurity and Infrastructure Security Agency (CISA) Cybersecurity Advisory Committee Designated Federal Officer, called the meeting to order. She provided a short summary of the *Federal Advisory Committee Act* rules governing the meeting and then turned the meeting over to the Honorable Jen Easterly, Director, CISA.

Director Easterly welcomed the attendees and introduced the Committee's new Chair, Mr. Tom Fanning, Southern Company, and Vice Chair, Mr. Ron Green, Mastercard. Mr. Fanning and Mr. Green then gave brief opening remarks. Mr. Fanning noted that it is both a moment of strategic risk and a moment of strategic opportunity for the United States and emphasized the need for the private sector and the government to work together to protect the Nation's interests. Mr. Ron Green added that the Committee creates an opportunity for a closer partnership between the private sector, industry, and academia.

Director Easterly then welcomed the Honorable John K. Tien, Deputy Secretary, Department of Homeland Security (DHS), to provide a keynote address.

Keynote Address

Deputy Secretary Tien applauded the diversity of viewpoints on the Committee and noted the importance of sharing wisdom, expertise, and insight from each area represented. He expressed his hope that the Committee will be able to help identify the gaps and vulnerabilities the United States currently faces and also provide solutions. He said that DHS is eager to hear the Committee's recommendations and that the members should challenge Director Easterly and all of DHS to take action on addressing the Nation's cybersecurity issues.

Director Easterly thanked Deputy Secretary Tien and introduced the Honorable Chris Inglis, National Cyber Director, to provide remarks.

Fortifying the Nation's Cybersecurity Posture

Director Inglis opened by stating that the United States needs to take the offensive in cyberspace and reframe what is believed to be possible and appropriate in terms of improving the resilience of the Nation's digital infrastructure. He added that, to address the current cyber threats, Government and industry need to do more than share information. He said that the Nation has an opportunity to develop a collective defense across Government, industry, and academia so that any attacker has to defeat the combined capabilities of all three adding that he is pleased with the work that CISA is doing in this regard. He charged the group to be proactive in showing that each member has something to add to the collaboration.

CISA's Big Challenges and Issues Tasking

Director Easterly stated that CISA has two important roles: 1) be the operational lead for federal cybersecurity; and 2) be the National Coordinator for Critical Infrastructure, Resilience and Security. She said that, of the two, she wants to focus on the critical infrastructure piece because the vast majority of critical infrastructure is

owned and operated by the private sector. To do this, she wants the Committee to provide input on how to move CISA from a focus on public-private partnerships to true operational collaboration.

Director Easterly noted that there are three efforts at CISA that she is particularly excited about. The first is the Joint Cyber Defense Collaborative (JCDC), which brings together the private sector along with the full power of Federal law enforcement, the Defense Department, and the Intelligence Community to address the cybersecurity threat in a proactive manner. The second effort is the CISA Cybersecurity Advisory Committee, which brings together strategic thinkers with a huge amount of expertise and experience and has the potential to magnify CISA's work collaboration and innovation and service to the nation. The third effort is the ongoing process of reshaping CISA's workforce through the Cyber Talent Management System.

Mr. Eric Goldstein, Assistant Director for Cybersecurity, CISA, discussed the need for greater visibility into the nation's critical infrastructure, noting that access to that information would allow CISA and other agencies to quickly develop actionable measures and actionable guidance that network defenders across the country can use to protect themselves before more intrusions occur. He emphasized that CISA cannot do this alone, and so the JCDC is building platforms where analysts from CISA as well as partners from Government and the private sector, potentially including cybersecurity companies, can work together to identify and collectively address threats across all of the networks they have visibility into.

Mr. Goldstein said that CISA plays a critical role in finding and fixing vulnerabilities, but that the only long-term solution is for the technology industry to adopt a more security-focused culture. He concluded by posing several questions to the Committee on how to address these issues: How can CISA shift the culture of technology more toward a security-focused model? How can CISA ensure that security features are easier to use and on by default? How can CISA and industry minimize the consequences of the use of technology in national critical functions?

Ms. Kiersten Todt, Chief of Staff, CISA, discussed CISA's efforts to build a strong cyber workforce, and how CISA can facilitate and drive that process. She noted that the agency is working to build relationships with non-traditional and underserved communities through partnerships with NPower, Girls Who Code, and the Cyber Warrior Foundation. Ms. Todt added that cyber is an interdisciplinary issue and the cyber workforce needs the skills of not just mathematicians, engineers and scientists, but also sociologists, psychologists, historians, politicians, and economists.

Director Easterly then turned to the first planned focus areas for the CISA Cybersecurity Advisory Committee: ***Transforming the Cyber Workforce***. She asked the members to provide their input. Ms. Lori Beer, JPMorgan Chase, said that employee retention is just as critical as creating a pipeline for entry level talent. She suggested that the Agency find a way to work with industry to provide corridors for employees to move back and forth between Government and industry. Ms. Nicole Wong, NWong Strategies, said two issues that stop candidates from working for the Government is its hierarchical nature and slow delivery process. She said this can frustrate cybersecurity specialists who are used to working with their company's leadership and moving fast to implement new ideas and solutions. Mr. Green said that MasterCard has a Cyber Talent Initiative that has MasterCard employees take positions in Government agencies for two-year terms to develop skills and knowledge that MasterCard cannot provide. He said this might be a model CISA could leverage. Mr. Ted Schlein, Kleiner Perkins Caufield & Byers, added that student loan relief would also be a big incentive to get candidates to join CISA and stay with the agency.

Director Easterly then moved to the topic ***Turning the Corner on Cyber Hygiene*** and asked Mr. George Stathakopoulos to give his thoughts. Mr. Stathakopoulos stated that it's almost impossible to ensure security across an entire supply chain as many small suppliers simply don't have the resources to address the issue. He said that, especially for small businesses, CISA needs to create a step-by-step guide to ensure these companies can provide at least the minimum level of security. Mr. Bobby Chesney, University of Texas, added that providing tax breaks to companies that work to improve cyber best-practices would also help. Ms. Suzanne Spaulding, Center for Strategic and International Studies, said that a long-term strategy would need to be education. Specifically, teaching civics so that children learn at a young age how their actions will impact others. Ms. Nicole Perlroth, Cybersecurity Journalist, added that using storytelling to explain how using multi-factor authentication

could have prevented major cyber-attacks could prove useful in this regard. Mr. Alex Stamos, Krebs Stamos Group, said that cloud providers should be required to include security features in their most basic sales packages. He noted that charging an additional fee to enable security creates a disincentive for customers to adopt these features. Mr. Green noted that mandates alone will not work, and that people need to be able to see the value of improving security. He suggested creating a cyber scorecard to grade companies on the cyber hygiene.

Director Easterly then asked Mr. Jeff Moss, DEF CON Communications, to discuss the topic of ***Igniting the Hacker Community***. Mr. Moss said that internet problems are global problems and addressing them will require global participation and a community response. He added that CISA should work to redefine the language around cybersecurity to make it clear how mutually beneficial it is. Mr. Moss noted health language works really well: If you're fighting against cancer, you're not fighting only for America. You're fighting against a global problem. He said that kind of inclusive language would get a lot more traction from the academic community. He added that hackers and academics need to provide an easy means for Government and policymakers to talk to them and receive feedback. Ms. Perlroth added that action is also important. She said it's important for CISA to think about its initial partnerships and ask: "Can CISA partner with the civil society community? Can CISA's efforts primarily support human rights defenders?" Ms. Marene Allison, Johnson & Johnson, noted that the Food and Drug Administration's process for working with the research community by creating a means for an open dialogue might provide CISA a model. Mr. Chris DeRusha, U.S. Chief Information Security Officer, Office of Management and Budget, added that CISA should consider reaching out to small groups like the Cyber Civilian Corps. Ms. Easterly said she would create a Technical Advisory Council as a subcommittee to address these issues.

On the topic of ***Protecting Critical Infrastructure from Misinformation & Disinformation***, Dr. Kate Starbird, University of Washington, noted that the level of disinformation being spread across information systems has been increasing dramatically in recent years. She noted that it was used in 2020 to undermine the U.S. election system and that it has also made it difficult for Governments to address crisis events like the COVID-19 pandemic. She said that the solution to addressing this is to teach people to care about whether what they're sharing is true or false. Mr. Chesney noted that it might be very difficult to get people to unlearn bad behavior like that as, after a while, it becomes an entrenched cognitive bias. He suggested that working with the various social media platforms to address the problem might be the best approach. Mr. Stamos and Ms. Allison noted that Government agencies are very bad at using their authority and platforms to push back against disinformation. Ms. Allison suggested that CISA create a playbook for agencies to use in responding to the spread of disinformation.

Director Easterly then turned to the topic of ***Building Resilience & Reducing Systemic Risk to Critical Infrastructure***. Mr. Fanning stated that one of the biggest impediments to industry and Government working together to address systemic risk is identifying the truly critical elements in critical infrastructure. He said CISA can help develop solutions, but that industry will need to take the lead in working with the Government to address the problem. Mr. Fanning noted that there are a number of models that CISA and industry could build on, such as the Analysis and Resilience Center for Systemic Risk developed by the Finance and Energy sectors. He closed by stating that, because industry controls the vast majority of critical infrastructure in the United States, the end goal should be for the Government to provide industry the tools to defend themselves.

Director Easterly recommended the following subcommittee assignments:

- **Transforming the Cyber Workforce**
 - Mr. Green, Mastercard (Lead)
 - Ms. Lori Beer, JPMorgan Chase
 - Ms. Nicole Perlroth, Cybersecurity Journalist
 - Dr. Pat Gallagher, University of Pittsburgh
 - Ms. Nicole Wong, NWong Strategies
 - Ms. Kiersten Todt, CISA

- **Turning the Corner on Cyber Hygiene**
 - Mr. George Stathakopoulos, Apple (Lead)
 - Mr. Steve Schmidt, AWS
 - Ms. Chris Young, Microsoft
 - Mr. Alex Stamos, Krebs Stamos Group
 - Mr. Ted Schlein, Kleiner Perkins
 - Ms. Nuala O'Connor, Walmart
 - Mr. Eric Goldstein, CISA
- **Igniting the Hacker Community (Technical Advisory Council)**
 - Mr. Jeff Moss, DEF Con Communications (Lead)
 - Mr. Kevin Mandia, Mandiant
 - Ms. Wong
 - Mr. Goldstein
 - Mr. Chris DeRusha, NCD/OMB
- **Protecting Critical Infrastructure from Misinformation & Disinformation**
 - Dr. Kate Starbird, University of Washington (Lead)
 - Ms. Suzanne Spaulding, Center for Strategic & International Studies
 - Mr. Matthew Prince, Cloudflare
 - Ms. Alicia Tate-Nadeau, State of Illinois
 - Ms. Vijaya Gadde, Twitter
 - Ms. Kim Wyman, CISA
 - Mr. Geoff Hale, CISA
- **Building Resilience & Reducing Systemic Risk to Critical Infrastructure**
 - Mr. Fanning (Lead)
 - Ms. Marene Allison, Johnson & Johnson
 - Mr. Bobby Chesney, University of Texas
 - Ms. Beer
 - Mr. Bob Kolasky, CISA
- **Strategic Communications**
 - Ms. Howe, Tenable (Chair)
 - Mayor Steve Adler, City of Austin
 - Mr. Schlein
 - Ms. Perlroth
 - Ms. Jen Easterly, CISA
 - Ms. Todt

Public Comment Period

Mr. Patrick Gaul, National Technology Security Coalition, provided the following comment for the record:

Good afternoon. This is Patrick Gaul. And as the Executive Director of the National Technology Security Coalition or the NTSC, the organization that spearheaded the creation of the Advisory Committee, and very proud and excited to see it operational. I'm eager to see the Advisory Committee demonstrate its value to Director Easterly, CISA, and the nation. I'm also proud that NTSC board members Marene Allison and Ron Green, are members of the Advisory Committee. Marene and Ron are preeminent in the field and I know their contributions will be vital. I'd also like to congratulate JPMorgan Chase and Microsoft, for their membership on the Advisory Committee, as they both have a board presence with the NTSC as well. As the only national organization representing the Chief Information Security Officer or CISO, we are eager to make our voices heard. CISOs work hard every day on the front lines, to combat cyber threats and maintain our collective national security. I believe there's no one who understands

cybersecurity better than those that practice it every day and who are also in the front of implementing national policy and regulatory requirements. In most large companies today the CISO role has become a member of the C-suite and the member trusted to protect the interests of the company and the customers. We look forward to watching the committee engage the cyber challenges ahead of us. We also sincerely hope, as the committee expands, more CISOs will have an opportunity to serve. And of course, the NTSC stands ready to support the committee. Thank you for allowing me to speak.

Closing Remarks and Adjournment

Director Easterly thanked the Committee members and other meeting participants for their input during the meeting. She also thanked the CISA and MITRE teams for supporting the meeting. She then gave each member an opportunity to ask any final questions. The Committee's Chair, Mr. Fanning, and Vice Chair, Mr. Green, both provided closing remarks noting that the Committee was off to a great start and that they looked forward to working on the issues discussed during the meeting. Director Inglis also thanked the Director and the participants, adding that he believed the Committee can make a serious dent in addressing the Nation's cybersecurity threats. Director Easterly adjourned the meeting.

APPENDIX

OPEN SESSION PARTICIPANT LIST

CSAC Members

Mr. Steve Adler	City of Austin, Texas
Ms. Marene Allison	Johnson & Johnson
Ms. Lori Beer	JPMorgan Chase
Mr. Robert Chesney	University of Texas
Mr. Thomas Fanning	Southern Company
Mr. Ron Green	Mastercard
Ms. Niloofar Razi Howe	Tenable
Mr. Kevin Mandia	Mandiant
Mr. Jeff Moss	DEF CON Communications
Ms. Nuala O'Connor	Walmart
Ms. Nicole Perlroth	Cybersecurity Journalist
Mr. Ted Schlein	Kleiner Perkins Caufield & Byers
Mr. Stephen Schmidt	Amazon Web Services
Ms. Suzanne Spaulding	Center for Strategic and International Studies
Mr. Alex Stamos	Krebs Stamos Group
Dr. Kate Starbird	University of Washington
Mr. George Stathakopoulos	Apple
Ms. Alicia Tate-Nadeau	Illinois Emergency Management Agency
Ms. Nicole Wong	NWong Strategies

Organization

Government Participants

The Hon. Jen Easterly	Cybersecurity and Infrastructure Security Agency (CISA)
The Hon. Chris Inglis	Office of the National Cyber Director (ONCD)
The Hon. John K. Tien	Department of Homeland Security (DHS)
Ms. Alaina Clark	CISA
Mr. Chris DeRusha	Office of Management and Budget
Ms. Osasu Dorsey	ONCD
Ms. Victoria Dillon	CISA
Mr. Jonathan Dunn	CISA
Mr. Eric Goldstein	CISA
Mr. Robert Kolasky	CISA
Mr. Brent Logan	CISA
Mr. Jason Mayer	DHS
Ms. Kaitlin Seale	CISA
Mr. Mark Stidd	CISA
Ms. Kiersten Todt	CISA
Ms. Megan Tsuyi	CISA
Ms. Kim Wyman	CISA

Organization

Other Attendees

Mr. Steve King

Contractor Support

Ms. Laura Karnas
 Mr. Barry Skidmore
 Ms. Quynh Tran
 Ms. Jennifer Peters

Dial-In Participants

Mr. Payton Alexander
 Mr. Lee Allen
 Ms. Denise Anderson
 Ms. Elizabeth Andrion
 Mr. Billy Anglin
 Ms. Felicia Archer
 Ms. Mariam Baksh
 Ms. Christina Berger
 Mr. Musadiq Bidar
 Mr. Christopher Bidwell
 Mr. Calvin Biesecker
 Ms. Ashley Billings
 Mr. Charles Blackmore
 Mr. Peter Bloniarz
 Mr. Per Brekke
 Ms. Cynthia Brumfield
 Mr. Brandon Buchanan
 Ms. Mary Byrd
 Ms. Courtney Callejas
 Ms. Genevieve Carnes
 Mr. Christopher Castelli
 Mr. Michael Chandaris
 Ms. Alicia Chavy
 Ms. Lodrina Cherne
 Ms. Ruth Clemens
 Mr. George Coleman
 Ms. Kathryn Condello
 Ms. Audrey Connors
 Mr. Justin Cooksey
 Ms. Bria Cousins
 Ms. Ann Cutler
 Ms. Jumoke Dada
 Mr. Raymond Decerchio

Organization

MITRE

Organization

Booz Allen Hamilton
 Insight
 Insight
 Nexight Group

Organization

Wiley Rein LLP
 TSA
 Health ISAC
 Charter Communications
 Sylint
 TSA
 Nextgov
 CISA SED
 CBS News
 Airports Council International
 Defense Daily
 CNN
 US Coast Guard
 Office of Governor New York
 Embassy of Norway
 CSO Online
 American Bus Association
 TSA
 US House of Representatives
 Association of American Railroads
 Booz Allen Hamilton
 TSA
 Beacon Global Strategies
 Cybereason
 CISA
 TSA
 Lumen
 Charter Communications
 Department of Energy
 CNBC
 CISA
 R Street Institute
 FAA

Dial-In Participants

Ms. Grace Dille
 Mr. Cameron Dixon
 Mr. Justin Doubleday
 Ms. Nzinga Dyson
 Mr. Obum Egolum
 Ms. Sharon Eshelman
 Ms. Katie Ewers
 Mr. Derrick Fail
 Ms. Michelle Feldstein
 Mr. Erik Fredrickson
 Ms. Sara Freidman
 Ms. Vijaya Gadde
 Mr. Rory Gallagher
 Mr. Michael Garcia
 Mr. Patrick Gaul
 Mr. Gregory Gavins
 Ms. Olivia Gazis
 Mr. Eric Geller
 Ms. Heather Gerard
 Ms. Leah Glaccum
 Ms. Tara Hairston
 Ms. Judith Harroun Lord
 Mr. Juan Hayes
 Ms. Katie Hazlett
 Mr. Andrew Hildick Smith
 Mr. Maurice Ed Hudson
 Mr. Michael Jacobs
 Mr. Eamon Javers
 Mr. Bob Joachim
 Mr. Lamar Johnson
 Mr. Derek Johnson
 Ms. Anne Johnson
 Ms. Jillian Joyce
 Mr. Albert Kammler
 Ms. Michealann Krause
 Ms. Norma Krayem
 Mr. Pradeep Kumar
 Mr. Jason Lamote
 Ms. Laura Laybourn
 Ms. Christina Lee
 Mr. Mark Lemmond

Organization

Meri Talk
 CISA
 Federal News Network
 Lewis Burke Associates LLC
 Capital One Financial
 Lewisburke Associates
 McKesson Corporation
 NOAA
 CISA OSPP
 Alaska Communications
 Inside Cybersecurity
 Twitter
 N/A
 Senate Homeland Security and Governmental Affairs
 National Technology Security Coalition
 Senate Homeland Security and Governmental Affairs
 CBS News
 POLITICO
 OASA ALT Army
 Defense Business Board
 Alliance for Automotive Innovation
 TSA
 TSA
 Commonwealth Strategic Partner
 Water ISAC
 CISA CSD
 TSA
 CNBC
 House Committee on Appropriations
 MeriTalk
 SC Media
 CISA CSD Contractor
 Committee on Homeland Security
 Van Scoyoc Associates
 Check Point Software Technologies
 Van Scoyoc Associates
 Tata Consultancy Services
 DHS Office of Legislative
 CISA NRMCC
 Beacon Global Strategies
 US Department of Energy

Dial-In Participants

Mr. Harry Lesser
 Mr. Devin Lynch
 Mr. Rafi Martina
 Ms. Tina Martinez
 Mr. Scott McConnell
 Mr. George McElwee
 Mr. Tim McGiff
 Mr. Michael McWilliams
 Ms. Ceydi Mendoza
 Ms. Maggie Miller
 Ms. Celinda Moening
 Ms. Valerie Mongello
 Mr. Drew Morin
 Ms. Stacy O'Mara
 Mr. James Orgill
 Ms. Cheri Pascoe
 Ms. Andrea Peterson
 Ms. Nancy Pomerleau
 Mr. Matthew Prince
 Mr. Donald Andy Purdy
 Ms. Kayla Renner
 Mr. Chris Riotta
 Mr. Michael Rosado
 Mr. Chris Rose
 Mr. Edward Rothgery
 Mr. Michael Ryan
 Ms. Farida Salama
 Ms. Geneva Sands
 Mr. Fred Schwien
 Mr. Tony Sibert
 Mr. Eric Snyderman
 Ms. Janet St. John
 Ms. Donna Steward
 Mr. Peter Su
 Mr. David Sucherman
 Mr. James Tollerson
 Mr. Costis Toregas
 Mr. Wesley Trimble
 Ms. Kimberly Underwood
 Mr. Christian Vasquez
 Mr. Joe Viens

Organization

OASA ALT Army
 SecurityScorecard
 Senate Select Committee on Intelligence
 CISA SED
 CISA
 Commonwealth Strategic Partner
 Venable LLP
 Defense Innovation Board
 DHS TSA
 The Hill
 N/A
 CISA
 Tmobile
 Mandiant
 Identification Technology Part
 NIST
 The Record
 CISA SED
 Cloudflare
 Huawei Technologies USA
 Monument Advocacy
 FCW
 Syntelligen Analytic Solutions
 CISA
 NSA
 US Coast Guard
 TSA
 CNN
 Boeing
 CosmGroup LLC
 CISA CSD
 Assoc of American Railroads
 Hi Trust Alliance
 Senate Homeland Security and Governmental Affairs
 CNBC
 Norfolk Southern
 Montgomery County MD and GW U
 Commonwealth Strategic Partner
 AFCEA International
 E&E News
 Charter Communications

Dial-In Participants

Ms. Andrea Vittorio
Ms. Bridgette Walsh
Mr. Jonathan Walton
Mr. Michael Widomski
Mr. David Wood
Ms. Orlie Natalie Yaniv
Mr. Darnell Young
Ms. Bridget Zamperini

Organization

Bloomberg News
Financial Services ISAC
TSA
CISA
CISA
Gigamon
TSA
Federal Transit Administration

CERTIFICATION

I hereby certify that, to the best of my knowledge, the foregoing minutes are accurate and complete.

Tom Fanning (approved on 18 December 2021)

Mr. Tom Fanning
CISA Cybersecurity Advisory Committee Chair

DEFENDANTS' EXHIBIT 122:

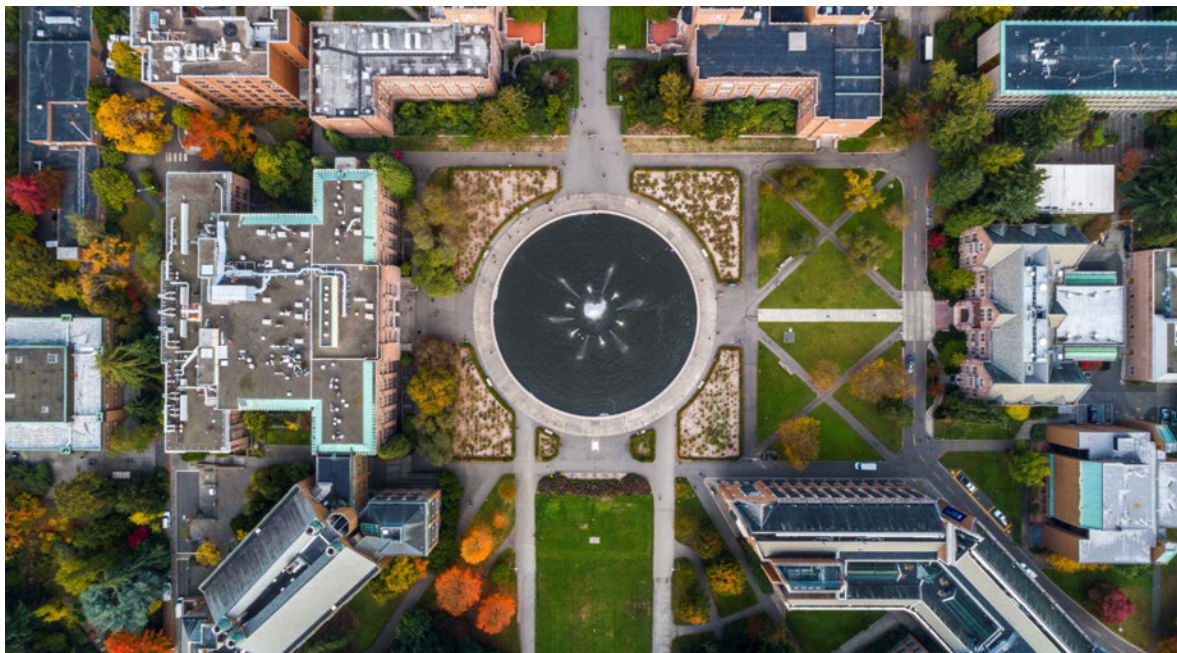


UNIVERSITY of WASHINGTON



Addressing false claims and misperceptions of the UW Center for an Informed Public's research

Mar 16, 2023



The researchers at the University of Washington's [Center for an Informed Public](#) (CIP) are recognized leaders in the study of rumors, conspiracy theories, and mis- and disinformation. Over the past decade, our research has made significant strides towards understanding and addressing these problems. Unfortunately, some of the projects CIP researchers have contributed to have become the subject of false claims and criticism that mischaracterizes our work, a tactic that peer researchers in this space are also experiencing. As mis- and disinformation researchers, it's distressing — though perhaps not surprising — to see some of the very dynamics and tactics we study being used to disrupt and undermine our own work and its impact. That includes our work with the nonpartisan [Election Integrity Partnership](#) research collaboration that we helped launch in 2020 with the [Stanford Internet Observatory](#) and other partners.

We're incredibly proud of our work. We appreciate the University of Washington's support as our team faces these [false claims](#) and [conspiracy theories](#).

The criticism of the CIP's research and team members is part of a larger effort that seeks to undermine work to understand and address online

misinformation, disinformation and other forms of strategic manipulation.

This effort aims to equate work to understand and address these challenges with “censorship” — functioning to cast doubt on research investigating mis- and disinformation and to undermine interventions that attempt to create more trustworthy information spaces. The rhetoric is similar to that employed in support of attempts to reframe the events of January 6, 2021, and to counter [the findings of the U.S. House’s select committee](#) that investigated what led to the violent attack that day on the U.S. Capitol.

One of the challenges of addressing misinformation is that corrections can often do more harm than good by bringing additional attention to false claims, and exposing new audiences. Indeed, it is [well established](#) that just hearing a false claim repeated, even within a correction, can make it more familiar, more memorable, and ultimately more believable for some audiences. Our team is very aware of the risks of giving oxygen to false claims. At the same time, we recognize the need to provide factual information that refutes some of the worst falsehoods and contextual information about how our work has been profoundly mischaracterized.

Our research team has been studying online rumors and conspiracy theories for a decade. One thing we have learned is that some of the most effective false narratives work not by spreading outright falsehoods, but by selectively seizing upon and mis-contextualizing bits of factual information, layering those with exaggerations and distortions to create a false impression. Unfortunately, these false impressions aren’t easily refuted through facts that counter individual claims. Often, those rebuttals just provide more ammunition for additional misrepresentations. So we thought we might take a slightly different tact and engage at the level of the false impression to explain how misperceptions of our work are being weaponized to fit into established political narratives.

False Impressions of the Election Integrity Partnership

Many of the misleading narratives and consequent misperceptions focus on our work with the [Election Integrity Partnership](#) (EIP). In the summer of 2020, researchers from the Stanford Internet Observatory (SIO), the University of Washington’s Center for an Informed Public (CIP), Graphika and the Digital Forensics Research Lab (DFRLab) embarked upon a collaborative “rapid-response” effort,

which would become known as the Election Integrity Partnership, to surface, analyze, and communicate about rumors and misleading claims about election processes and procedures.

False impression: *CIP researchers were acting outside of the mission of the university.*

In mid-July of 2020, researchers at Stanford pitched the EIP to our team at the University of Washington's Center for an Informed Public as a collaboration between four research organizations who would share resources and expertise to help identify and address the spread of harmful false and misleading information that might threaten the integrity of the U.S. election. As university researchers, we are encouraged both to contribute to scientific knowledge and to have "broader impact" on society. For example, CIP co-founder Kate Starbird participated, both as a PhD student and UW faculty member, in real-time "crisis mapping" projects that used crowdsourcing techniques to support disaster response after the Haiti earthquake, during the Deepwater Horizon oil spill, and around dozens of other events. The UW CIP team has specialized skills in social media data analysis and in July 2020, we accepted the invitation to join the EIP, offering to provide data analysis and communication support to the project. **Our participation in the EIP directly aligns with the CIP's public service mission and the UW's commitment to public scholarship.**

False impression: *The EIP is a partisan political project.* This incorrect impression stems from an attempt to frame the empirical findings of the EIP — i.e., that misleading claims about election processes and results spread more among Republicans than Democrats — as reflecting political motives of the partnership's mission. When we agreed to join, we ensured the effort was explicitly non-partisan.

Plans included collaboration with an office within the Trump Administration (the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency) and outreach to both major political parties, who were invited to contribute to a crowdsourced tip-line. **The founding mission of the EIP focused on protecting the integrity of elections, not on supporting any specific political outcome.** The EIP's work sought to mitigate the impact of false claims that might interfere with election processes as well as false claims about election interference. After the events of the 2016 election, we believed this mission to be a nonpartisan one.

False impression: The EIP was a “secret” project. This false impression first emerged in summer 2022 after online activists purported to “discover” the EIP’s work — in a [peer-reviewed paper](#). This delayed discovery was not due to any nefarious effort by the EIP to obscure our work. On the contrary, we made every effort to share the products of our work and to accurately describe the processes underneath. In the weeks leading up to and following the November 2020 election, we published [a number of blog posts, graphics and data visualizations](#) showing how certain misleading narratives spread online, hosted news briefings, and fielded numerous interview requests from news organizations. In March 2021, our team published [“The Long Fuse: Misinformation and the 2020 Election,”](#) a nearly 300-page report that, in addition to describing our methods, documented the narratives and information dynamics of the “Big Lie.” We are incredibly proud of this research, which is part of the historical record, cited in the [U.S. House select committee’s final report](#) into what led to the January 6, 2021, attack on the U.S. Capitol. Our efforts from 2020 led to follow-up peer-reviewed research published in journals and conferences, including [Nature Human Behaviour](#). And the paper that was “discovered” in the summer of 2022 was published in an open journal and promoted through our CIP website and social media accounts. **The EIP’s work was conducted openly and transparently.**

False impression: The EIP was a “censorship” operation. At the core of most of the false impressions of our work is a rhetorical argument that seeks to equate efforts to understand and counter false and misleading information with “censorship.” This argument has increasingly been employed against social media moderation efforts — as though these companies do not routinely act to limit spam, pornography, harassment, impersonation, and other harmful content on their networks. In 2020, some social media platforms put into place “civic integrity” policies to mitigate the spread of false claims about the 2020 election, including content that could disenfranchise voters by confusing them about when or where to vote and content that delegitimized election results. One dimension of the EIP’s work was to alert social media platforms to misleading claims about election processes, discovered in the course of our analysis efforts, that may have violated their policies. Our understanding is that the social media platforms the EIP worked with provide similar reporting mechanisms for other researchers and organizations, in part because they do not currently have the internal capacity or expertise to do that work alone. Platforms also provide reporting mechanisms for all users to utilize should they

encounter content that goes against community guidelines. The EIP's reports to the platforms were voluntary contributions to these companies efforts to mitigate election misinformation, and the platforms were not bound to act on the recommendations of our researchers. **We disagree with the framing of the EIP's work as "censorship" — and are troubled by broader efforts to equate research about misinformation and disinformation with "censorship."**

False impression: *The EIP orchestrated a massive "censorship" effort.* In a recent tweet thread, Matt Taibbi, one of the authors of the "Twitter Files" claimed: "According to the EIP's own data, it succeeded in getting nearly 22 million tweets labeled in the runup to the 2020 vote." That's a lot of labeled tweets! **It's also not even remotely true.** Taibbi seems to be conflating our team's post-hoc research mapping tweets to misleading claims about election processes and procedures with the EIP's real-time efforts to alert platforms to misleading posts that violated their policies. The EIP's research team consisted mainly of non-expert students conducting manual work without the assistance of advanced AI technology. **The actual scale of the EIP's real-time efforts to alert platforms was about 0.01% of the alleged size.**

False impression: *The EIP's purpose was to route moderation requests from outside organizations to social media platforms.* This misimpression relies on three distortions of our reported work. First, though the EIP reported content to platforms, **alerting platforms to content that violated their policies was only a small part of the EIP's mission** — and not equally shared across the four collaborating teams. Other activities included publicly communicating in "real time" about misleading claims and narratives through tweets and blog posts, documenting the wide range of misleading claims and narratives about the election in our final report, and publishing a dataset mapping tweets to hundreds of distinct claims. Second, though the EIP included a "crowdsourced" tip-line where external partners could share pieces of content for us to consider for review, our researchers made independent decisions about what to pass on to platforms, just as the platforms made their own decisions about what to do with our tips. Third, the **majority** of our work focused on content surfaced by our own, internal research team. **The EIP's purpose was to support U.S. democracy through independently organized efforts to identify, analyze, document, communicate about, and correct false rumors and disinformation about election processes and procedures.**

False impression: *The EIP operated as a government cut-out, funneling censorship requests from federal agencies to platforms* This impression is built around falsely framing the following facts: the founders of the EIP consulted with the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) office prior to our launch, CISA was a "partner" of the EIP, and the EIP alerted social media platforms to content EIP researchers analyzed and found to be in violation of the platforms' stated policies. These are all true claims — and in fact, we reported them ourselves in the EIP's March 2021 final report. But the false impression relies on the omission of other key facts. **CISA did not found, fund, or otherwise control the EIP. CISA did not send content to the EIP to analyze, and the EIP did not flag content to social media platforms on behalf of CISA.**

False impression: *The EIP collaborated with and worked to support the Biden Administration* This impression builds upon documentation of the EIP's partnership with CISA (an office that sits within the Executive Branch of government) and is used to promote a "weaponization of government" narrative aimed at the Biden Administration. However, this is easily corrected by a glimpse at the timeline. The EIP was founded in 2020 and its collaboration with the CISA office took place between July 2020 and November 2020. During that time, CISA was run by an appointee of President Trump. CISA's association with the EIP was reviewed and approved by Trump Administration attorneys as compatible with CISA's congressionally approved authorities. **When the EIP collaborated with an organization within the Executive Branch of the U.S. government (CISA), it was during the Trump Administration.**

False impression: *Researchers at the University of Washington were paid and directed by the U.S. government in their work with the EIP.* This misimpression builds from factual, public information about UW researchers' federal grant funding, but integrates a mischaracterization of this funding being designated for EIP operations and conflates those operations with "censorship." It then expands to include a false allegation that the agencies within the U.S. government and specifically the National Science Foundation (NSF) intentionally funded the University of Washington to "censor" specific voices. In 2020, UW participation in the EIP was predominantly funded by foundational and philanthropic funding. UW personnel funded by Kate Starbird's NSF CAREER grant did participate in post-election period analysis of EIP data for the partnership's final report and for subsequent peer-reviewed publications — and that grant is publicly acknowledged in that work. However,

research grants from the U.S. government did not significantly fund nor did U.S. government funding agencies direct or encourage participation by UW students, staff, or faculty in the platform-alerting functions of the EIP.

False impression: *The EIP purposefully targeted conservative political speech.* This false impression is created by underemphasizing the narrow scope of our research and highlighting specific elements of our empirical research findings (that more misinformation spread on the political right) without context (that these findings are unsurprising and align with [other research](#)). The EIP's work was narrowly focused on content that 1) interfered with voting by misleading about when or where to vote; 2) encouraged others to commit fraud; 3) used intimidation or threats of violence to deter voting; or 4) delegitimized election results through the spread of false, misleading, or unsubstantiated claims. In the lead up to the 2020 election, the EIP reported on misleading claims spreading through left leaning audiences as well as right-leaning ones (e.g., [here](#) and [here](#)). After the election, the vast majority of false claims about the election emerged and spread among supporters of President Trump (a fact underscored by the January 6 violence at the U.S. Capitol), which is reflected in our data and reporting **The EIP exclusively tracked and reported on false, misleading, and unsubstantiated claims about election processes and procedures. In 2020, those claims were far more prominent among supporters of President Trump (and the president himself) than other political groups.**

False impression: *The EIP orchestrated content moderation decisions by social media platforms around the story of Hunter Biden's laptop.* This false impression has few facts or even details behind it, but takes shape through repeated speculation and insinuation **The story of Hunter Biden's laptop was out of scope for the EIP's work and the EIP did not play any role in: 1) decisions by Twitter (or any other platform) to limit spread of the laptop story; or 2) attributions of the laptop story to foreign influence operations.**

False Impressions of Dr. Kate Starbird's work on CISA's external advisory committee

In December 2021, CIP co-founder and faculty director Kate Starbird, a UW Human Centered Design & Engineering associate professor, was asked by CISA Director Jen Easterly to serve on CISA's external advisory committee (CSAC) — and to chair the MDM subcommittee. "MDM" is an acronym used by the U.S. government to refer to misinformation, disinformation, and malinformation. Starbird agreed to chair the

MDM committee, which released a first set of recommendations in June 2022, and a second set of recommendations in September 2022, concluding the committee's work.

False impression: *Members of CISA's MDM advisory subcommittee worked as part of a "censorship regime "* This false impression combines the argument that "moderation equals censorship" with false speculation about the nature of the MDM subcommittee's work. **The MDM subcommittee did not participate in or recommend for others to participate in any activities related to social media platform moderation or other activities that could be construed, even broadly, as "censorship."** The subcommittee was initially tasked with addressing — through written recommendations — challenging questions about how CISA should structure their work, engage with external stakeholders, and address privacy concerns related to addressing mis- and disinformation. The subcommittee limited the scope of their work to the context of elections. The subcommittee's recommendations focused not on how government or platforms should limit communication, but on how the CISA office should use their own communication, for example through public awareness campaigns, debunking falsehoods, and helping to amplify factual information from local and state election officials. The subcommittee did not recommend or discuss what actions social media platforms should take pertaining to specific content or types of content. Subcommittee members Kate Starbird and Vijaya Gadde did not discuss activities that platforms have taken or should take regarding specific content or policies more generally — neither within their roles on the committee or outside them. **The CSAC MDM subcommittee did not discuss whether or how social media platforms should moderate content, either in specific cases or more generally.**

False impression: *CISA's MDM subcommittee recommended that the federal government participate in monitoring of social media platforms and other information spaces* This misimpression emerged following an unfortunate November 2, 2022, article in The Intercept that included a misleading edit and broader mischaracterization of the subcommittee and its work. The article stated that the subcommittee had recommended CISA to "*closely monitor* 'social media platforms of all sizes, mainstream media, cable news, hyper partisan media, talk radio and other online resources.'" To be clear, **the MDM subcommittee explicitly never advocated for CISA to monitor or "closely monitor" anything.** During internal discussions, the members noted that questions about social media monitoring by

CISA and other government offices were beyond the capacity of the subcommittee and, though initially tasked with providing recommendations on that aspect of CISA's work, the subcommittee intentionally did not provide recommendations about this. The Intercept added "closely monitor" to a section of the report that was instead encouraging CISA to consider the challenge of MDM as broader than just social media. **This misleading misquote of the report has contributed to a lasting, widespread, and harmful misperception about the MDM subcommittee's work.**

What comes next and what's at stake?

At the University of Washington's Center for an Informed Public, our research team has developed unique expertise, including methods and infrastructure, for rapid analysis of social media information flows during fast-paced and high-visibility events. Our researchers have a long track record of studying rumors, conspiracy theories and mis- and disinformation that not only pre-dates the formation of the Election Integrity Partnership in 2020, but also our own research center, which was established at the University of Washington in 2019. This vital work will continue.

As [multiple public opinion polls](#) show, Americans are very concerned about mis- and disinformation, which can be harmful in certain contexts and lead to poor decision making during crises and emergencies. Disinformation can manipulate individuals and societies in harmful ways. Pervasive disinformation can undermine our trust in information, in science, in our foundational institutions, and in each other. Online mis- and disinformation have real-life consequences, as we saw on January 6, 2021.

Our work at the CIP, including our Election Integrity Partnership collaboration in 2020, has been transparent, research-driven, and rooted in support for democracy and support for a more informed public. This is the CIP's mission. This work will continue. We're currently working on a final report around our research on the 2022 U.S. midterm elections, expected for release in the coming months, but you can explore [blog posts and other analysis we published](#) and [shared via Twitter](#) last fall.

As researchers who study the dynamics of rumors, conspiracy theories, and mis- and disinformation online, we're well familiar with Brandolini's Law, or the [bullshit asymmetry principle](#) where the "amount of energy needed to refute bullshit is an

order of magnitude bigger than to produce it.” As we’ve been responding to this slurry of false claims, distortions and misunderstandings, we’ve learned that all the attention on our research and researchers underscores their importance and impact. We will continue to stand behind and defend our work.

Kate Starbird

Associate Professor, University of Washington Human Centered Design & Engineering

Co-Founder and Director, UW Center for an Informed Public

Ryan Calo

Professor, UW School of Law and UW Information School

Co-Founder, UW Center for an Informed Public

Chris Coward

Senior Principal Research Scientist, UW Information School

Co-Founder, UW Center for an Informed Public

Emma S. Spiro

Associate Professor, UW Information School

Co-Founder, UW Center for an Informed Public

Jevin D. West

Associate Professor, UW Information School

Co-Founder, UW Center for an Informed Public

Other News



A chatbot exercise in ‘BSing the BS principle’

Apr 4, 2023

In a March 31 opinion in The Seattle Times about AI chatbots, University of Washington Center for an Informed Public co-founder Jevin West says that chatbots will be “vectors of propaganda,” make it harder to discern truth and further erode trust in institutions.

[Read More](#)

Responding to recent questions about Kate Starbird’s participation on a CISA external advisory committee

Apr 4, 2023

Over the past several months, our team at the University of Washington Center for an Informed Public has been responding to inquiries related to our research and UW associate professor Kate Starbird’s participation on an external advisory committee for the Cybersecurity and Infrastructure Security Agency (CISA)

[Read More](#)



At MisinfoDay 2023 events across Washington, high school students and educators learn valuable skills

Mar 28, 2023

Approximately 700 Washington high school students, teachers, librarians and other educators participated in MisinfoDay 2023 programs in March across three in-person events at the University of Washington in Seattle and Washington State University in Pullman and Vancouver.

[Read More](#)

[Join our Mailing List](#)

[Contact Us](#)

[Privacy Policy](#)

[Terms and Conditions](#)



© 2021 Center for an Informed Public at UW

DEFENDANTS' EXHIBIT 123:



CISA CYBERSECURITY ADVISORY COMMITTEE

SUBCOMMITTEE FACTSHEET

Background

The CISA Cybersecurity Advisory Committee has established six subcommittees to study various aspects of CISA's cybersecurity efforts:

- Transforming the Cyber Workforce;
- Turning the Corner on Cyber Hygiene;
- Technical Advisory Council;
- Protecting Critical Infrastructure from Misinformation and Disinformation;
- Building Resilience and Reducing Systemic Risk to Critical Infrastructure; and
- Strategic Communications

Subcommittees

- **Transforming the Cyber Workforce**
 - Purpose: Will focus on building a comprehensive strategy recommendation to identify – and develop – the best pipelines for talent, expand all forms of diversity, and develop retention efforts to keep our best people. We will also aim to find creative ways to educate communities “K through Gray” to develop a better-informed digital workforce and to inspire the next generation of cyber talent.
 - Chair: Ron Green
 - CSAC Members: Nicole Perlroth, Nicole Wong, and Chris Young
- **Turning the Corner on Cyber Hygiene**
 - Purpose: Will help determine how Government and industry can collaborate to identify appropriate goals and ensure strong cyber hygiene is easy to execute.
 - Chair: George Stathakopoulos
 - CSAC Members: Bobby Chesney, Nuala O'Connor, Matthew Prince, Steve Schmidt, and Alex Stamos
- **Technical Advisory Council**
 - Purpose: Will be comprised of hackers, vulnerability researchers, and threat intelligence experts to get direct feedback from front-line practitioners whose work is vital to the security of our nation
 - Chair: Jeff Moss
 - Subcommittee Members: Dino Dai Zovi, Luiz Eduardo, Isiah Jones, Kurt Opsahl, Runa Sandvik, Yan Shoshitaishvili, Rachel Tobac, David Weston, Bill Woodcock, and Yan Zhu
- **Protecting Critical Infrastructure from Misinformation and Disinformation**
 - Purpose: Will evaluate and provide recommendations on potentially effective critical infrastructure related counter-MDM efforts that fit within CISA's unique capabilities and mission.
 - Chair: Kate Starbird
 - CSAC Members: Vijaya Gadde, Suzanne Spaulding, and Alicia Tate-Nadeau
- **Building Resilience and Reducing Systemic Risk to Critical Infrastructure**
 - Purpose: Will help to determine how to best drive national risk management and determine the criteria for scalable, analytic model to guide risk prioritization.
 - Chair: Tom Fanning
 - CSAC Members: Marene Allison, Lori Beer, and Kevin Mandia
- **Strategic Communications**
 - Purpose: Will focus on evaluating and making recommendations on expanding CISA's reach with critical partners to help build a national culture of cyber resilience. The subcommittee will provide recommendations to help promote CISA as a willing and collaborative partner, working arm-in-arm with partners to understand, manage, and reduce risk to our cyber and physical infrastructure. SC will highlight CISA's partners and showcase the success that comes from collaboration.
 - Chair: Niloofar Razi Howe
 - CSAC Members: Steve Adler, Nicole Perlroth, and Ted Schlein



AMERICA'S CYBER DEFENSE AGENCY

SHARE:    

PUBLICATION


2022 Cybersecurity Advisory Committee (CSAC) Reports and Recommendations


Publish Date: March 06, 2023





View the collection of reports and recommendations published by the CISA Cybersecurity Advisory Committee.

Resource Materials

 **June 2022 CSAC Recommendations - CH** [</sites/default/files/2023-03/csac_june-quarterly-meeting-recommendations_ch.pdf>](/sites/default/files/2023-03/csac_june-quarterly-meeting-recommendations_ch.pdf)
(PDF, 216.46 KB)

 **June 2022 CSAC Recommendations - MDM** [</sites/default/files/2023-03/csac_june-quarterly-meeting-recommendations_mdm.pdf>](/sites/default/files/2023-03/csac_june-quarterly-meeting-recommendations_mdm.pdf)
(PDF, 233.25 KB)

 **June 2022 CSAC Recommendations - SC** [</sites/default/files/2023-03/csac_june-quarterly-meeting-recommendations_sc.pdf>](/sites/default/files/2023-03/csac_june-quarterly-meeting-recommendations_sc.pdf)
(PDF, 171.34 KB)

 **June 2022 CSAC Recommendations - TAC**
[</sites/default/files/publications/june%25202022%2520csac%2520recommendations%2520%25e2%2580%2593%2520tac.pdf>](/sites/default/files/publications/june%25202022%2520csac%2520recommendations%2520%25e2%2580%2593%2520tac.pdf)
(PDF, 332.29 KB)



June 2022 CSAC Recommendations - TCW

</sites/default/files/publications/june%25202022%2520csac%2520recommendations%2520-%2520tcw.pdf>
(PDF, 228.51 KB)



Formal Director's Response to June 2022 Recommendations

/sites/default/files/2023-03/formal_response_to_cisa_cybersecurity_advisory_committee_recommendations_june_2022%20%282%29.pdf
(PDF, 221.54 KB)



CSAC September 2022 Recommendations MDM

/sites/default/files/2023-02/csac_september_recommendations_mdm.pdf
(PDF, 93.88 KB)



CSAC September 2022 Recommendations - SR

/sites/default/files/2023-03/csac_september_recommendations_sr%20%281%29.pdf
(PDF, 186.99 KB)



Formal Director's Response to September 2022 Recommendations

/sites/default/files/2023-03/csac_september-quarterly-meeting-recommendations_dir-response_2023-03-01_508_v2_0.pdf
(PDF, 182.27 KB)



CSAC 2022 Annual Report

/sites/default/files/2023-03/csac_december-quarterly-meeting_tab-09_annual-report_2022-11-30%20%282%29.pdf
(PDF, 271.51 KB)

Critical Infrastructure Security and Resilience </topics/critical-infrastructure-security-and-resilience>

Partnerships and Collaboration </topics/partnerships-and-collaboration>

Cyber Threats and Advisories </topics/cyber-threats-and-advisories>

Related Resources

PUBLICATION

CISA Cybersecurity Advisory Committee (CSAC) Fact Sheet </resources/tools/resources/cisa-cybersecurity-advisory-committee-csac-fact-sheet>

MAR 20, 2023 ■ PUBLICATION

Cybersecurity Advisory Committee (CSAC) Subcommittee Fact Sheet </resources-

[tools/resources/cybersecurity-advisory-committee-csac-subcommittee-fact-sheet>](#)

MAR 13, 2023 ■ MEETING AGENDAS

CISA Cybersecurity Advisory Committee (CSAC) Meeting Resources </resources-

[tools/resources/cisa-cybersecurity-advisory-committee-csac-meeting-resources>](#)

JAN 27, 2023 ■ PUBLICATION

Secure Your Drone: Privacy and Data Protection Guidance </resources-tools/resources/secure-your-

[drone-privacy-and-data-protection-guidance>](#)

[Return to top](#)

Topics </topics>

Spotlight </spotlight>

Resources & Tools </resources-tools>

News & Events </news-events>

Careers </careers>

About </about>



**CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY**



CISA Central

888-282-0870

Central@cisa.dhs.gov

CISA.gov

An official website of the U.S. Department of Homeland Security

[About CISA </about>](#)

[Accessibility <https://www.dhs.gov/accessibility>](https://www.dhs.gov/accessibility)

[Budget and Performance <https://www.dhs.gov/performance-financial-reports>](https://www.dhs.gov/performance-financial-reports)

[DHS.gov <https://www.dhs.gov>](https://www.dhs.gov)

[FOIA Requests <https://www.dhs.gov/foia>](https://www.dhs.gov/foia)

[No FEAR Act </cisa-no-fear-act-reporting>](#)

[Office of Inspector General <https://www.oig.dhs.gov/>](https://www.oig.dhs.gov/)

[Privacy Policy </privacy-policy>](#)

[Subscribe](#)

[The White House <https://www.whitehouse.gov/>](https://www.whitehouse.gov/)

[USA.gov <https://www.usa.gov/>](https://www.usa.gov/)

[Website Feedback </forms/feedback>](#)

DEFENDANTS' EXHIBIT 124:



**CISA
CYBERSECURITY
ADVISORY
COMMITTEE**

REPORT TO THE CISA DIRECTOR

Protecting Critical Infrastructure from Misinformation and Disinformation

Information Sharing Around Foreign Adversary Threats to Elections

September 13, 2022

Introduction:

The Protecting Critical Infrastructure from Misinformation and Disinformation (MDM) Subcommittee submitted a first set of recommendations in June 2022. The recommendations outlined below aim to emphasize and add further detail to key points and provide additional items for consideration.

Findings:

In 2017-2018, in the wake of revelations of persistent social media manipulation by Russia-affiliated organizations such as the Internet Research Agency, there was widespread concern about foreign disinformation operations targeting U.S. audiences — especially in the context of elections. In more recent years, attention has shifted to domestic sources of disinformation, but there are reasons to anticipate that the elections in 2022 and 2024 may again attract significant foreign sources of potential interference. With the U.S. providing significant aid to Ukraine and imposing strong economic sanctions against Russia, the Russian government has every incentive to disrupt the upcoming elections in ways that will exacerbate existing mistrust of the process and potentially cause the kind of chaos that can lead to political violence. China, too, may have an incentive to interfere in the U.S. elections as a response to what they see as provocations regarding Taiwan or to further their narrative that U.S. democracy is chaotic and corrupt. The U.S. federal government, state and local election officials, the courts, social media platforms, traditional media, and other relevant organizations should all prepare for significant information operations, including those enabled by malicious cyber activity (whether successful or merely noisy attempts), from Russia, China, and other adversaries.

If the objective of adversary operations targeting elections is to exacerbate a lack of trust in the process, foreign attacks on U.S. election infrastructure are likely to involve two integrated attack vectors. Similar to a “hack-and-leak” operation, we might term this type of attack a “hybrid cyber-misinformation and disinformation (MDM)” attack. The first vector involves attempting to infiltrate (i.e., hack) that infrastructure to cause damage by changing voter rolls or votes (a traditional cybersecurity threat to a critical function). The second involves information operations to draw attention to infiltration (even if attempted hacks were unsuccessful) or broader information operations designed to undermine trust in the process, thereby undermining the critical function of elections. It is therefore important to prepare for, detect, and respond to these operations holistically — along both their cybersecurity and information dimensions.

Recommendations:

Stemming from these insights, we have the following recommendations outlined below:

- **Share information with state and local election officials.** CISA should work with the Intelligence Community (IC), including the Federal Bureau of Investigation, to ensure that the information needs of election officials around foreign disinformation threats are prioritized. To identify the intelligence requirements of local and state election officials, CISA should work with the Elections Infrastructure Government Coordinating Council (GCC). In particular, the CSAC believes that providing information and assistance to the many local elections officials across the country is critical, not just secretaries of state or election officials at the state level. Considering the fundamental importance of elections, CISA should ensure that intelligence information about adversary activity related to elections is promptly shared with state and local elections officials with as much



**CISA
CYBERSECURITY
ADVISORY
COMMITTEE**

detail as possible, including attribution, consistent with protection of sources and methods.

- **Protect the courts.** Given the essential role courts play in ensuring the resolution of disputes about the election process and ensuring the peaceful transfer of power, they, too, may be the target of an intensified campaign to undermine public trust in the legitimacy of their processes. CISA should consider the following two recommendations that:
 - Relevant information around foreign hacking and disinformation attacks are shared with the courts; and
 - The IC includes adversary activity targeting the courts in the collection and analysis priorities related to elections.



**CISA
CYBERSECURITY
ADVISORY
COMMITTEE**

Supporting State and Local Elections Officials

September 13, 2022

Introduction:

The MDM Subcommittee submitted a first set of recommendations in June 2022. The recommendations outlined below aim to emphasize and add further detail to key points and provide additional items for consideration.

Findings:

CISA should continue to provide resources for state and local election officials to support their efforts to address misinformation and disinformation (MDM) targeting their jurisdictions. State and local election officials are first-hand sources for information about elections. CISA should support their efforts to effectively communicate accurate information and actively counter inaccurate information about their election materials and processes.

Recommendations:

1. At the highest level, CISA should share up to date “best practices” around how to proactively address and counter MDM based on the most recent research. To help election officials craft their messaging, CISA should provide templates and customizable content that local and state election officials can adapt to their specific needs. A particular need for many local and state election officials is around establishing a website. CISA should provide resources, including templates and grants for technical support — e.g., to create and maintain websites to host election-related resources for their constituents. CISA has a massive audience and communication resources and should leverage both to amplify content — including accurate information about election materials and procedures — from local and state election officials.
2. CISA must ensure that there is a national effort to bring insights together on an ongoing basis, and to share tools, training, and templates. Elections are ultimately local and must be managed locally. That said, some of these disinformation campaigns are likely to use similar tactics, techniques, and messaging aimed at multiple jurisdictions.
3. CISA's role in this whole-of-nation effort to counter adversary information operations around upcoming elections should be consistent with this Subcommittee's earlier recommendations, with a focus on furthering CISA's existing mission. Within the federal government, the intelligence community is likely to have the best insights on foreign adversary activity. CISA's role should be to ensure that those insights are promptly provided to state and local election officials. CISA should also consider unique aspects of foreign information operations when developing tools, templates, and training for those officials.

DEFENDANTS' EXHIBIT 125:



Home Blog Election 2020



Oct 5, 2022

A Statement from the Election Integrity Partnership

There has been a lot of recent interest in the work of the Election Integrity Partnership, and we are thrilled that a much larger audience of citizens is interested in hearing about our efforts to detect and research election-related disinformation. Unfortunately, not everything written or said on TV about us has been correct, so we wanted to present some basic facts:

- **The Election Integrity Partnership is a non-partisan collaboration with a tightly defined mission to find and investigate false rumors and disinformation about election processes and procedures.**

Evaluating claims about candidates, their positions, and political parties – whether true or false – is not part of EIP’s mission. Our focus, as described in multiple posts and our final report, has been on identifying attempts to interfere in the running of an election, to encourage fraud, or to delegitimize the results using false or misleading claims. For example, the controversy over Hunter Biden’s laptop is an example of a topic that would not be in scope for EIP, and we had no part in the discussion around the appropriate treatment of that story. A table from our final report:

A grid showing the four categories of election disinformation in scope for the EIP, from The Long Fuse: Misinformation and the 2020 Election (stanford.edu)

- **The Election Integrity Partnership has always operated openly and transparently.** We published multiple public blog posts in the run-up to the 2020 election, hosted daily webinars immediately before and after the election, and published our results in a 290-page final report and multiple peer-reviewed academic journals. Any insinuation that information about our operations or findings were secret up to this point is disproven by the two years of free, public content we have created.
- **The Cybersecurity and Infrastructure Security Agency (CISA) was created by the CISA Act,** passed unanimously by both houses of Congress and signed by President Trump in November 2018. Its mission is to protect critical infrastructure (including that around elections) in the United States from cyber threats — including both hacking and what the federal government refers to as “MDM” (misinformation, disinformation, and malinformation). A core part of CISA’s work is forging collaborations between government and industry to help defend our critical infrastructure against cybersecurity threats. CISA’s website describes how the organization connects “stakeholders in industry and government to each other and to resources, analyses, and tools to help them build their own cyber, communications, and physical security and resilience, in turn helping to ensure a secure and resilient infrastructure for the American people.”
- **EIP’s partnership with CISA began under the Trump administration.** The EIP partnered with CISA in 2020, both to help them understand rumors and disinformation around the 2020 election and so CISA could provide corrective and/or clarifying information from election officials. At the time of that partnership, the agency was run by an appointee of President Trump, and CISA’s relationship with EIP was reviewed and approved by Trump Administration attorneys as compatible with CISA’s congressionally approved authorities.
- **CISA did not send any examples of potential misinformation to EIP.** EIP was in contact with the nearly 10,000 bipartisan local election officials around the country via the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC). Local officials of either or no party could send issues to EIP for us to investigate so they could respond to disinformation through the media or CISA via the “Rumor Control” website. *To be clear, EIP did not send any reports of false rumors or disinformation to social media companies on behalf of the Department of Homeland Security or the Cybersecurity and Infrastructure Security Agency.*
- **Most incidents EIP analyzed were discovered internally.** Though EIP allowed several outside groups to send in reports of potential election disinformation, the vast majority (79%) of the incidents we investigated were first discovered by our own analysts. External reports generated tickets that were investigated by our analysts in the same manner as potential disinformation discovered internally. The judgment of whether something qualified as mis- or disinformation and was “in scope” for our project was made by EIP’s leadership, and information that was sent to us was not treated differently than any report generated internally by our analysts.

- **Social-media platforms, not EIP, decided which action to take.** The EIP collected examples of falsehoods about the election into consolidated reports and, when we believed that these falsehoods violated the policies of social media platforms, we sent along our reports. Each company made their own determinations on how to treat our reports. Here is an example of one of those reports, drawn from our public report of March 2021:

A screenshot of a ticket reporting the Sharpiegate misinformation to several platforms, from The Long Fuse: Misinformation and the 2020 Election (stanford.edu)

The EIP was able to communicate with a bipartisan group of local election officials on this issue via the E-ISAC. After our referral, many examples of the false “Sharpiegate” rumors continued to exist on social media (and still do) but were possibly labeled or demonetized.

- **Both the Republican National Committee and Democratic National Committee were invited to submit tickets.** We offered a wide set of organizations the ability to send in potentially false claims for us to investigate, including both the Republican and Democratic National Committees. The Republican National Committee was contacted on July 28, 2020. They did not respond to our inquiry and did not submit any referrals.
- **The Democratic National Committee ended up sending four reports to the EIP:**
 - One report involved a claim about voting-by-mail that received little traction and was closed without action.
 - One report was for a political ad on Facebook that made false claims about vote-by-mail fraud in an attempt to raise money. This ad was identical to an ad that had already been disabled by Facebook and was referred to Facebook as such.
 - One report listed several spammy content farms with extreme political content. The majority of the content was not within the tight scope of the EIP and discarded, and a handful of posts were monitored but did not have significant traction. No referrals were made to social media platforms.
 - One report led our team to discovering two linked Facebook pages attempting to mislead American voters using Facebook Ads. One of these ads incorrectly claimed that completed ballots had been thrown out. We alerted Facebook to this ad, and they suspended it. We observed that even after being suspended, shares of the ad remained visible and unlabeled on the platform. This investigation was immediately written up in this blog post.
- **One ticket was sent to the DNC to enlist their help in stopping election misinformation being spread by Democrats.** The EIP received reports from the Maryland State Board of Elections and the National Association of State Election Directors that a graphic containing incorrect vote-by-mail request deadlines had been shared by Democratic party affiliates; the DNC was tagged to alert them to the mistakes in the content as EIP analysts looked into the material. A follow-up indicated that Facebook had been independently notified and took action on the posts with incorrect dates.
- **An NAACP referral exposed a false claim against the Proud Boys.** We also reached out to multiple civil society groups concerned with election rumors in their communities, including the NAACP. There was only one referral from the NAACP, expressing concern about their membership receiving threatening emails that claimed to be sent by the Proud Boys on behalf of President Trump. We immediately investigated both the emails and a related video, which claimed to show Proud Boys hackers creating fake mail-in ballots to rig the

election for President Trump. During our analysis, we discovered discrepancies in the video that proved that the targets for this attack were not actually U.S. election systems but a virtual machine hosted in Moldova. We immediately sent our analysis to the team at CISA, who forwarded it to the FBI and other government agencies. Soon afterward, a united team of leadership from across the Trump Administration announced that this campaign had originated in Iran, and two Iranian individuals have since been indicted for attempting to interfere in the U.S. election. We are pleased to have played a small role in helping prevent Iranian agents from creating a false belief that President Trump was stealing the 2020 election in concert with the Proud Boys. We promptly shared our research in a blog post here.

- **Claims that our work was designed to target conservative voices are false.** Contrary to assertions that we ignored false rumors and disinformation on the political left, we worked hard to be balanced in our work. We reported on election rumors and disinformation targeting and spreading within Democrat-voting audiences — for example, in a blog post that covered rumors emerging from criticism of the U.S. Postal Service. However, the vast majority of false rumors and disinformation about the 2020 election spread primarily through far-right influencers catering to Trump-voting audiences, reflecting the asymmetrical nature of the phenomenon. Our research — which has been peer-reviewed in academic journals and aligns with other research and reporting by journalists and news organizations — reflects that trend.
- **The EIP does not “target” individual influencers, but we do factually report on their impact.** Through careful analysis of hundreds of “incidents” of false/misleading claims, our research team identified high-profile accounts of media and political figures who were repeatedly influential in the spread of false and misleading claims questioning the integrity of the 2020 U.S. election. We identified a similar list of media domains that were similarly influential in the spread of false and misleading election claims. These lists were not provided directly to any partner organization. We published them through our website, public presentations, our “Long Fuse” report, and most recently in a peer-reviewed paper — as well as a statement to the U.S. House Select Committee on the January 6 Attack on the United States Capitol.
- **Claims that the Biden Administration funded the EIP and that the research funding we have received was motivated by the federal government seeking to censor specific voices are patently false.**
 - The operations of the EIP are primarily funded through philanthropic grants to partner organizations. However, the work of the EIP generated a rich dataset for research into the spread of rumors and disinformation, and some of the post hoc work analyzing the data generated by the EIP has been funded by the National Science Foundation, initially through a grant to study online disinformation that preceded the formation of the EIP and now through a grant that specifically supports this research.
 - In August 2021, the National Science Foundation, through its Secure and Trustworthy Cyberspace (SaTC) program, awarded a \$3 million collaborative grant to a team led by the University of Washington and Stanford University for research that is developing and evaluating “rapid response” methods for studying and communicating about disinformation at a sophistication and pace on par with the dynamic and interdisciplinary nature of the challenge, like that currently being done through our research partnership. This grant supports translating the EIP’s work into research contributions,

including frameworks for other groups to use to identify, analyze, and communicate about disinformation.

- Our researchers have a long track record of receiving research funding from the National Science Foundation to study online rumoring and disinformation. Our application to the NSF was reviewed by a panel of outside experts and awarded based on the strength of the research. Any claim that the funding of this work emerged as a “reward” for “censoring” specific voices or a commitment to do the same in the future, is false.

As researchers who spend our days dealing with false claims, propaganda, and disinformation, we are not surprised when our work is targeted, including by some of the same people and organizations who are weakening American democracy by spreading or supporting baseless claims of non-existent election fraud. Dealing with such false claims is a part of doing this research. But in the wake of these false reports, members of our team, which includes students, have received threatening emails and social media messages for participating in an academic research project. That isn't right.

There has also been some interest expressed in our work by members of Congress. Several of our leaders have testified repeatedly on these topics, and we would be happy to return to Congress to discuss our work and how domestic disinformation actors are damaging the long-term health of American democracy.

The EIP is continuing its nonpartisan and collaborative work in the 2022 election cycle. Our aim is not to fact-check, nor to decide what is or isn't “misinformation.” We aim to understand how bad-faith actors manipulate the information environment, how corrections flow through the network, and how genuine confusions might be reduced. Our mission is to pass our insights on to the public and our partners to strengthen our shared democracy.

Thank you for your interest in the work of the Election Integrity Partnership.

< Voting Rights Legislation
Framed to Support Election
Conspiracy Theories About
Non-citizens Voting

10 Factors That Shape a
Rumor's Capacity for Online
Virality

>

DEFENDANTS' EXHIBIT 126:



U.S. DEPARTMENT *of* STATE



About Us



GLOBAL ENGAGEMENT CENTER

Mission: To direct, lead, synchronize, integrate, and coordinate U.S. Federal Government efforts to recognize, understand, expose, and counter foreign state and non-state propaganda and disinformation efforts aimed at undermining or influencing the policies, security, or stability of the United States, its allies, and partner nations.

Vision: To be a data-driven body leading U.S. interagency efforts in proactively addressing foreign adversaries' attempts to undermine U.S. interests using disinformation and propaganda.

The GEC carries out its mission along five lines of effort:

- 1. Analytics and Research:** GEC's analysts and data scientists collect and analyze data from foreign state and foreign non-state actors to produce analysis on their foreign malign information influence narratives, tactics, and techniques. GEC shares these analyses with stakeholders within the Department, and among S. embassies, the interagency, and our international partners.
- 2. International Partnerships:** GEC has built and participates in multiple international coalitions and partnerships with other national governments for the purpose of coordinating counter-disinformation analyses and actions, and collectively buttressing the integrity of the global information environment.

3. **Programs and Campaigns:** GEC's Russia, People's Republic of China, Iran, and Counterterrorism teams each designed to build societal and institutional resilience to foreign propaganda and disinformation efforts abroad. GEC tailors its initiatives to the specific challenges in unique overseas information environments and coordinates both internally within the Department, and with interagency and international partners.
4. **Exposure:** GEC plays a coordination role in the interagency's public exposure of foreign information influence operations, including the use of proxy sites and social media networks overseas.
5. **Technology Assessment and Engagement:** GEC hosts private sector technology demonstrations, assesses counter-disinformation technologies against specific challenges, and identifies technological solutions through technology challenge programs.

Establishment of the Global Engagement Center: GEC's founding traces back to 2011 and Executive Order 13584, which established within the Department of State the Center for Strategic Counterterrorism Communications (CSCC) for the purpose of "supporting agencies in Government-wide public communications activities targeted against violent extremism and terrorist organizations."^[1] Executive Order 13721 in 2016 transformed the CSCC into the Global Engagement Center but left its counterterrorism mission largely unchanged.

GEC's mission expanded upon enactment of the *National Defense Authorization Act for Fiscal Year 2017* to include the authority to address other foreign state and non-state propaganda and disinformation activities. The *John S. McCain National Defense Authorization Act for Fiscal Year 2019* further refined this mission, and endowed it with a mandate, as reflected in GEC's mission statement.^[2]

[1] *John S. McCain National Defense Authorization Act for Fiscal Year 2019*, Section 1284, Modifications to Global Engagement Center, P.L. 115-232, <https://www.congress.gov/bill/115th-congress/house-bill/5515/text>

[2] The White House Office of the Press Secretary, Executive Order 13584-Developing an Integrated Strategic Counterterrorism Communications Initiative, September 9, 2011, <https://obamawhitehouse.archives.gov/the-press-office/2011/09/09/executive-order-13584-developing-integrated-strategic-counterterrorism-c>

TAGS

Data

Disinformation



U.S. DEPARTMENT *of* STATE

White House

USA.gov

Office of the Inspector General

Archives

Contact Us



Privacy Policy

Accessibility Statement

Copyright Information

FOIA

No FEAR Act

DEFENDANTS' EXHIBIT 127:

2018 WL 2933298 (D.O.J.)

Department of Justice (D.O.J.)

National Security Division (NSD)

(NEWS RELEASE)

DEPUTY ASSISTANT ATTORNEY GENERAL ADAM S. HICKEY TESTIFIES BEFORE
SENATE JUDICIARY COMMITTEE AT HEARING TITLED “ELECTION INTERFERENCE:
ENSURING LAW ENFORCEMENT IS EQUIPPED TO TARGET THOSE SEEKING TO DO HARM”

June 12, 2018

Good morning, Chairman Grassley, Ranking Member Feinstein, and distinguished Members of the Committee. Thank you for the opportunity to testify on behalf of the Department of Justice concerning our efforts to combat election interference.

The Attorney General identified this issue as a priority when he created a Cyber-Digital Task Force earlier this year and directed it to address “efforts to interfere with our elections,” among other threats. That Task Force is expected to submit a report to the Attorney General by the end of this month and will issue a public report in mid-July. The Department appreciates the Committee's interest in making sure that law enforcement has the tools we need to target those who may seek to do us harm by interfering in our elections.

As I describe below, the Department's principal role in combatting election interference is the investigation and prosecution of Federal crimes, but our investigations can yield more than criminal charges to protect national security. Foreign influence efforts extend beyond efforts to interfere with elections, and they require more than law enforcement responses alone. I will cover three areas in my testimony today. First, I will describe what we mean by the term “foreign influence operations” and provide examples of operations we have observed in the past. Second, I will discuss how the Department has categorized recent foreign influence operations targeting our elections. Third, and finally, I will explain how the Department is responding to those operations and how our efforts fit within the “whole of society” approach that is necessary to defeat foreign influence operations.

1. Background on Foreign Influence Operations

Foreign influence operations include covert actions by foreign governments intended to affect U.S. political sentiment and public discourse, sow divisions in our society, or undermine confidence in our democratic institutions to achieve strategic geopolitical objectives.

Foreign influence operations aimed at the United States are not a new problem. These efforts have taken many forms across the decades, from funding newspapers and forging internal government communications, to more recently creating and operating false U.S. personas on Internet sites designed to attract U.S. audiences and spread divisive messages. The nature of the problem, however - and how the U.S. government must combat it - are changing as advances in technology allow foreign actors to reach unprecedented numbers of Americans covertly and without setting foot on U.S. soil. Fabricated news stories and sensational headlines like those sometimes found on social media platforms are just the latest iteration of a practice foreign adversaries have long employed in an effort to discredit and undermine individuals or organizations in the United States.

Although the tactics have evolved, the goals of these activities remain the same: to spread disinformation and to sow discord on a mass scale in order to weaken the U.S. democratic process, and ultimately to undermine the appeal of democracy itself.

As one deliberate component of this strategy, foreign influence operations have targeted U.S. elections. Indeed, elections are a particularly attractive target for foreign influence campaigns because they provide an opportunity to undermine confidence in a core element of our democracy: the process by which we select our leaders. As explained in the January 2017 report

by the Office of the Director of National Intelligence (ODNI) addressing Russian interference in the 2016 U.S. presidential election, Russia has had a “longstanding desire to undermine the U.S.-led liberal democratic order,” and that nation's recent election-focused “activities demonstrated a significant escalation in directness, level of activity and scope of effort compared to previous operations.” Russia's foreign influence campaign, according to ODNI, “followed a Russian messaging strategy that blends covert intelligence operations - such as cyber activity - with overt efforts by Russian Government agencies, state-funded media, third-party intermediaries, and paid social media users or ‘trolls.’”

Although foreign influence operations did not begin and will not end with the 2016 election, the operations we saw in 2016 represent a significant escalation in the directness, level of activity and scope of efforts aimed at the United States and our democracy, based in large part on the utility of the Internet for conducting these operations. They require a strong response.

2. Types of Foreign Influence Operations

In advance of the 2018 mid-term elections, the Department is mindful of ODNI's assessment that Russia, and possibly other adversaries, likely will seek to interfere in the 2018 midterm elections through influence operations. Such operations could include a broad spectrum of activity, which we categorize as follows. Importantly, these categories are just a way to conceptualize the types of foreign influence activity our adversaries might engage in; they are not an indication that foreign governments actually have engaged in each described category of activity.

1. Cyber operations targeting election infrastructure. Such operations could seek to undermine the integrity or availability of election-related data. For example, adversaries could employ cyber-enabled or other means to target election infrastructure, such as voter registration databases and voting machines. Operations aimed at removing otherwise eligible voters from the rolls or attempting to manipulate the results of an election (or even just disinformation suggesting that such manipulation has occurred), could undermine the integrity and legitimacy of elections, as well as public confidence in election results. To our knowledge, no foreign government has succeeded in perpetrating ballot fraud, but raising even the doubt that it has occurred could be damaging.

2. Cyber operations targeting political organizations, campaigns, and public officials. These operations could seek to compromise the confidentiality of private information of the targeted groups or individuals, as well as its integrity. For example, adversaries could conduct cyber or other operations against U.S. political organizations and campaigns to steal confidential information and use that information, or alterations thereof, to discredit or embarrass candidates, undermine political organizations, or impugn the integrity of public officials.

3. Covert influence operations to assist or harm political organizations, campaigns and public officials. For example, adversaries could conduct covert influence operations to provide assistance that is prohibited from foreign sources to political organizations, campaigns and government officials. These intelligence operations might involve covert offers of financial, logistical, or other campaign support to, or covert attempts to influence the policies or positions of, unwitting politicians, party leaders, campaign officials, or even the public.

4. Covert influence operations, including disinformation operations, to influence public opinion and sow division. Using false U.S. personas, adversaries could covertly create and operate social media pages and other forums designed to attract U.S. audiences and spread disinformation, or divisive messages. These messages need not relate directly to campaigns. They may seek to depress voter turnout among particular groups, encourage third-party voting, or convince the public of widespread voter fraud in order to undermine confidence in election results.

5. Overt influence efforts, such as the use of foreign media outlets or other organizations to influence policymakers and the public. For example, adversaries could use state-owned or state-influenced media outlets to reach U.S. policymakers or the public. Governments can disguise these outlets as independent, while using them to promote divisive narratives and political objectives.

3. The Department of Justice's Role in Addressing Foreign Influence Operations

The Department of Justice has a significant role in investigating and disrupting foreign government activity inside the United States that threatens U.S. national security. With both law enforcement and intelligence authorities, the FBI is the lead federal agency responsible for investigating foreign influence operations, and the Department's prosecutors are responsible for charging and prosecuting any federal crimes committed during a foreign influence operation. The FBI has established the Foreign Influence Task Force (FITF) to identify and combat foreign influence operations targeting U.S. democratic institutions, with focus on the U.S. electoral process and the 2018 and 2020 elections. Through our own authorities and in close coordination with our partner Departments and agencies, the Department can act against threats posed by foreign influence operations in several ways.

First, as an intelligence-driven organization and member of the Intelligence Community (IC), the FBI can pursue tips and leads, including from classified information, to investigate illegal foreign influence activities and, in coordination with the IC and the Department of Homeland Security, share information from those investigations with State and local election officials, political organizations, and others to help them detect, prevent, and respond to computer hacking, espionage, and other criminal activities.

Second, through the FITF, the Department maintains strategic relationships with social media providers, who bear the primary responsibility for securing their own products, platforms and services from this threat. By sharing information with them, the FBI can help providers with their own initiatives to track foreign influence activity and to enforce terms of service that prohibit the use of their platforms for such activities. This approach is similar to the Department's approach in working with social media providers to address terrorists' use of social media.

Third, the Department's investigations may expose conduct that warrants criminal charges. Criminal charges are a basic tool the Department uses to pursue justice and deter similar conduct in the future. We work with other nations to obtain custody of foreign defendants whenever possible, and those who seek to avoid justice in U.S. courts will find their freedom of travel significantly restricted. Criminal charges also provide the public with information about the activities of foreign actors we seek to hold accountable and raise awareness of the threats we face.

Fourth, the Department's investigations can support the actions of other U.S. government agencies using diplomatic, intelligence, military, and economic tools. For example, in several recent cases, the Secretary of the Treasury has imposed financial sanctions on defendants abroad under executive orders that authorize the imposition of sanctions for malicious cyber-enabled activity. (See [E.O. 13694 \(Apr. 1, 2015\)](#), as amended by [E.O. 13757 \(Dec. 29, 2016\)](#).) Treasury's action blocked all property and interests in property of the designated persons subject to U.S. jurisdiction and prohibited U.S. persons from engaging in transactions with the sanctioned individuals.

Finally, in appropriate cases, information gathered during our investigations can be used - either by the Department or in coordination with our U.S. government partners - to alert victims, other affected individuals, and the public to foreign influence activities. Exposure of foreign influence operations ultimately may be one of the best ways to counter them. Victim notifications, defensive counterintelligence briefings and public safety announcements are traditional Department activities, but they must be conducted with particular sensitivity in the context of elections, to avoid even the appearance of partiality.

In taking these actions, we are alert to ways in which current law may benefit from reform. By providing ready access to the American public and policymakers from abroad, the Internet makes it easier for foreign governments to evade restrictions on undeclared domestic activities and mask their identities while reaching an intended audience. We welcome the opportunity to work with Congress to combat foreign influence operations, including those aimed at our elections, by clarifying or expanding our laws to provide new tools or sharpen existing ones, if appropriate.

4. Conclusion

The nature of foreign influence operations will continue to change as technology and our foreign adversaries' tactics continue to change. Our adversaries will persist in seeking to exploit the diversity and richness of today's information space, and the tactics and technology they employ will continue to evolve.

The Department plays an important role in combating foreign efforts to interfere in our elections. At the same time, it cannot and should not attempt to address the problem alone. There are limits to the Department's role - and the role of the U.S. government more broadly - in addressing foreign influence operations aimed at sowing discord and undermining our institutions. Combating foreign influence operations requires a “whole of society” approach that relies on coordinated actions by Federal, State, and local government agencies; support from the private sector; and the active engagement of an informed public.

I want to thank the Committee again for providing me this opportunity to discuss these important issues on behalf of the Department. We look forward to continuing to work with Congress to improve our ability to respond to this threat. I am happy to answer any questions you may have.

2018 WL 2933298 (D.O.J.)

End of Document

© 2023 Thomson Reuters. No claim to original U.S. Government Works.

DEFENDANTS' EXHIBIT 128:

2018 WL 3727551 (D.O.J.)

Department of Justice (D.O.J.)

National Security Division (NSD)

(NEWS RELEASE)

DEPUTY ASSISTANT ATTORNEY GENERAL ADAM S. HICKEY FOR THE
NATIONAL SECURITY DIVISION DELIVERS REMARKS AT MISINFO CON

August 6, 2018

Remarks as prepared for delivery

Thank you for the invitation to speak today, and for the important work you are doing: in organizing this conference devoted to the challenges of misinformation, and, by attending, bringing your experience and expertise to bear on the problem.

It's a privilege to help kick off this first day of MisinfoCon, focused on state-sponsored misinformation. To do that, I am going to give you an overview of how the Department of Justice views the problem, where it fits in the context of related national security threats, and how we are addressing it.

As you probably know, the Justice Department recently obtained an indictment of 13 Russian individuals and three entities, including the Internet Research Agency (or IRA), for federal crimes in connection with an effort to interfere in the 2016 Presidential election. The defendants allegedly conducted what they called “information warfare against the United States,” with the stated goal of “spread[ing] distrust towards the candidates and the political system in general.”

According to the indictment, the IRA was a structured organization headed by a management group and arranged in departments. It had a “translator project,” designed to focus on the U.S. population, with more than 80 employees assigned by July 2016. They posed as politically and socially active Americans, advocating for and against particular political candidates. They established social media pages and groups to communicate with unwitting Americans. They also purchased political advertisements on social media.

One of the so-called trolls who worked for the IRA recently spoke to the Washington Post about his work in a different department, attempting to influence a domestic, Russian audience. He described it as “a place where you have to write that white is black and black is white.” Hundreds of people “were all writing absolute untruths.”

But as the indictment alleges it, what made the defendants' conduct illegal in the United States was not the substance of their message, the “accuracy” of their opinions: it was their conspiracy to defraud by, among other ways, lying about who the messenger was. They were not Americans expressing their own viewpoints; they were Russians on the payroll of a foreign company.

Now, the problem of covert foreign influence is not new. In 1938, a congressional committee found that the Nazi government had established an extensive, underground propaganda apparatus inside the United States using American firms and citizens. The response was to recommend a law that would (in the committee's words) throw these activities under the “spotlight of pitiless publicity.” The result is the Foreign Agents Registration Act (FARA), a disclosure statute that, notably, does not prohibit speech. Rather, FARA requires agents of foreign principals who engage in political activities within the United States to file periodic public disclosures with the Department.

The Act's purpose is to ensure that the American public and our lawmakers know the source of information provided at the behest of a foreign principal, enhancing the public's and the government's ability to evaluate such information.

Transparency, not prohibition, has been the government's response to misinformation. In the 1980s, the government established an interagency committee, the "Active Measures Working Group," to counter Soviet disinformation. It did so by exposing forgeries and other propaganda, such as fake stories that the Pentagon developed the AIDS virus as part of a biological weapons research program.

Today, we confront misinformation as only one component of a broader, malign foreign influence effort. As this framework from the Department's recent Cyber-Digital Task Force report shows, those efforts can also include cyber operations that target election infrastructure or political parties' networks; covert efforts to assist (or harm) candidates; and overt efforts to influence the American public (for example, through state-run media organizations).

Our responses to those efforts must likewise be multifaceted, from providing indicators and warnings that can help network owners protect themselves from hackers, to criminal investigations and prosecutions, and other measures, like sanctions and expulsions that raise the costs on the states that sponsor such malign activities.

This graphic, also from the Task Force report, depicts the Department's strategy to counter each phase of a covert influence campaign cycle, from the identification of targets to the production and amplification of content. The middle rows (in red) depict our adversaries' activities in stages, while the bottom rows (in blue) suggest the means by which private actors and the government can disrupt and deter the activity.

One aspect of this strategy worth highlighting is that the content of a foreign influence campaign may be true or false. Whether the message is accurate or not may not be the point: doxing a candidate or a corporation for political reasons might not involve misinformation, but it may nonetheless violate our laws, threaten our values and way of life, compromise privacy and, sometimes, retaliate against and chill free speech.

Covert foreign influence efforts can take many forms, but recently we have seen increased efforts to influence Americans through social media. To counter these efforts, a key component of our approach is sharing information with social media and other Internet service providers, which we do through the FBI's Foreign Influence Task Force. It is those providers who bear the primary responsibility for securing their own products and platforms. By sharing information with them, especially about who certain users and account holders actually are, we can assist their own, voluntary initiatives to track foreign influence activity and to enforce their own terms of service.

As the Task Force report also recognizes, there may be circumstances when it is appropriate for the government itself to expose and attribute foreign influence operations as a means of rendering them less effective. But there are often compelling, countervailing considerations, however.

As a general rule, the Department does not confirm, deny, or comment on pending investigations, both to protect the investigation itself as well as the rights of any accused.

We are also constrained to protect the classified sources and methods that may inform our judgment of what foreign governments are doing.

And, most important of all, we must never act to confer any advantage or disadvantage on any political or social group, individual, or organization, and we must strive to avoid even the appearance of partiality. That could constrain the timing and nature of any disclosure we might make.

All of this is to say, and as the Department's Policy on the Disclosure of Foreign Influence Operations recognizes, we might not be the best messenger to counter a particular piece of misinformation.

That's why this conference is so important: what we call the private sector (but which includes a lot of people in public spaces, just like you) has a critical role - larger than the federal government's - in countering covert foreign influence efforts, particularly misinformation, and ensuring that our democracy rests on the active engagement of an informed public.

The former Russian troll I mentioned at the beginning of my remarks, who worked for the IRA, said his work was “pointless” for Russian audiences, that it would not impact them. But in America, that kind of trickery might have an impact, he said, because we “live in a society in which it's accepted to answer for your words.” My challenge to us during this conference, if I may make one, is that we find ways to ensure we all continue to answer for our words, so that the trust we enjoy as an aspect of our free, democratic society can thrive.

2018 WL 3727551 (D.O.J.)

End of Document

© 2023 Thomson Reuters. No claim to original U.S. Government Works.